2025



Handbook For Investigating Officers

Procedure To Handle Data Disclosure Requests To Social Media Intermediaries

IFSO, Special Cell, Delhi Police

Handbook for Investigating Officers: Process for Data Disclosure Requests from Social Media Intermediaries

Index

Chapter 1- Introduction.....1

Chapter 2- Meta Platforms, Inc.....6

Chapter 3- WhatsApp LLC. 15

Chapter 4- X (Twitter) Corp.....24

Chapter 5- Reddit, Inc.....39

Chapter 6- LinkedIn Corporation.....50

Chapter 7- Google LLC. 66

Chapter 8- Telegram FZ-LLC 74

Chapter 9- Information Furnished 76

Chapter 10- Dos and Don’ts.....78

Chapter 1- Introduction

During the hearing of Writ Petition W.P.(Crl.) 1563/2024 titled Shabana versus GNCT Delhi and Ors., the Hon'ble Delhi High Court directed the Delhi Police vide order dated 13.11.2024 to coordinate with Social Media Intermediaries (*hereinafter referred as SMIs*) platforms and to take steps towards preparing a handbook. This handbook is to be used and disseminated to all police stations that may require urgent information from these platforms.

Objective

The objective of the handbook is to serve as a comprehensive guide for Investigating Officers (*hereinafter referred to as IOs*) outlining the process of obtaining data disclosure from SMIs, as per the procedures they laid down.

Legal Compliance

The handbook highlights key legal provisions, including the Information Technology Act, 2000, *hereinafter referred to as IT Act*, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, *hereinafter referred to as IT Rules* and relevant sections of the Bharatiya Nagarik Suraksha Sanhita (BNSS), to ensure compliance and avoid procedural lapses.

Consistency and Standardization

The handbook standardises data disclosure requests to social media intermediaries for uniformity across Delhi Police. It includes interfaces, templates, checklists, and examples, specifying required details like case references, specific data sought, and legal basis.

Efficiency and Timeliness

Considering the volume of requests being generated from Delhi Police Investigating Officers (IOs), the handbook aims to help create an escalation matrix for each SMI to efficiently and timely dispose of data disclosure requests.

Awareness

The handbook aims to increase awareness among IOs about how these platforms operate and the types of data they can provide.

Conclusion

By achieving these objectives, the handbook aspires to establish a robust framework for IOs, ensuring that data disclosure requests from SMIs are handled with precision, legality, and efficiency, ultimately aiding the pursuit of justice in the digital age.

Legal Provisions

1. **Sec. 94 of BNSS, 2023: Summons to produce document or other thing**
   (1) Whenever any Court or any officer in charge of a police station considers that the production of any document, electronic communication, including communication devices, which is likely to contain digital evidence or other things is necessary or desirable for the purposes of any investigation, inquiry, trial or other proceeding under this Sanhita by or before such Court or officer, such Court may issue a summons or such officer may, by a written order, either in physical form or in electronic form, require the person in whose possession or power such document, or thing is believed to be, to attend and produce it, or to produce it, at the time and place stated in the summons or order.
   (2) Any person required under this section merely to produce a document or other thing shall be deemed to have complied with the requisition if he causes such

document or thing to be produced instead of attending personally to produce the same.

2. ***Rule 3(1)(d) of IT Rules-*** As per this rule, the intermediary shall remove the unlawful content, as early as possible, but in no case later than thirty-six hours from the receipt of order from the court or the notified or the Designated Officer.
3. ***Rule 3(1)(g) of IT Rules, 2021 –*** As per this rule, any information which has been removed or access to which has been disabled, the intermediary shall, without vitiating the evidence in any manner, preserve such information and associated records for one hundred and eighty days for investigation purposes, or for such longer period as may be required by the court or by Government agencies who are lawfully authorised.
4. ***Rule 3(1)(h) of IT Rules, 2021 –*** As per this rule, where an intermediary collects information from a user for registration on the computer resource, it shall retain his information for a period of one hundred and eighty days after any cancellation or withdrawal of his registration, as the case may be.
5. ***Rule 3(1)(j) of IT Rules, 2021 –*** As per this rule, the intermediary shall, as soon as possible, but not later than seventy two hours and in case of an online gaming intermediary who enables the users to access any permissible online real money game not later than twenty-four hours, of the receipt of an order, provide information under its control or possession, or assistance to the Government agency which is lawfully authorised for investigative or protective or cyber security activities, for the purposes of verification of identity, or for the prevention, detection, investigation, or prosecution, of offences under any law for the time being in force, or for cyber security incidents:

   Provided that any such order shall be in writing stating clearly the purpose of seeking information or assistance, as the case may be.

6. ***Rule 4(1)(a) of the IT Rules, 2021*** – As per this rule, the social media intermediary shall appoint a Chief Compliance Officer who shall be responsible for ensuring compliance with the Act and rules made thereunder and shall be liable in any proceedings relating to any relevant third-party information, data or communication link made available or hosted by that intermediary where he fails to ensure that such intermediary observes due diligence while discharging its duties under the Act and rules made thereunder:

   Provided that no liability under the Act or rules made thereunder may be imposed on such significant social media intermediary without being given an opportunity of being heard.

   Explanation – For the purposes of this clause "Chief Compliance Officer" means a key managerial personnel or such other senior employee of a significant social media intermediary (SSMI) who is resident in India.

7. ***Rule 4(1)(b) of the IT Rules, 2021*** – As per this rule, the social media intermediary shall appoint a nodal contact person for 24x7 coordination with law enforcement agencies and officers to ensure compliance to their orders or requisitions made in accordance with the provisions of law or rules made thereunder.

   Explanation- For the purposes of this clause "nodal contact person" means the employee of a significant social media intermediary, other than the Chief Compliance Officer, who is resident in India.

8. **Section 84(b) of the IT Act, 2000 – Punishment for abetment of offences**

   Whoever abets any offence shall, if the act abetted is committed in consequence of the abetment, and no express provision is made by this Act for the punishment of such abetment, be punished with the punishment provided for the offence under this Act.

Explanation – An act or offence is said to be committed in consequence of abetment, when it is committed in consequence of the instigation, or in pursuance of the conspiracy, or with the aid which constitutes the abetment.

9. **Section 84(c) of the IT Act, 2000 – Punishment for attempt to commit offences** Whoever attempts to commit an offence punishable by this Act or causes such an offence to be committed, and in such an attempt does any act towards the commission of the offence, shall, where no express provision is made for the punishment of such attempt, be punished with imprisonment of any description provided for the offence, for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence, or with both.

   If the social media intermediary fails to submit the requisite information within the prescribed time frame of 36 hours, he shall be penalized under Section 84(b) of the IT Act or Section 84(c) of IT Act, (as the case may be), read with Rule 7 of IT Rules.

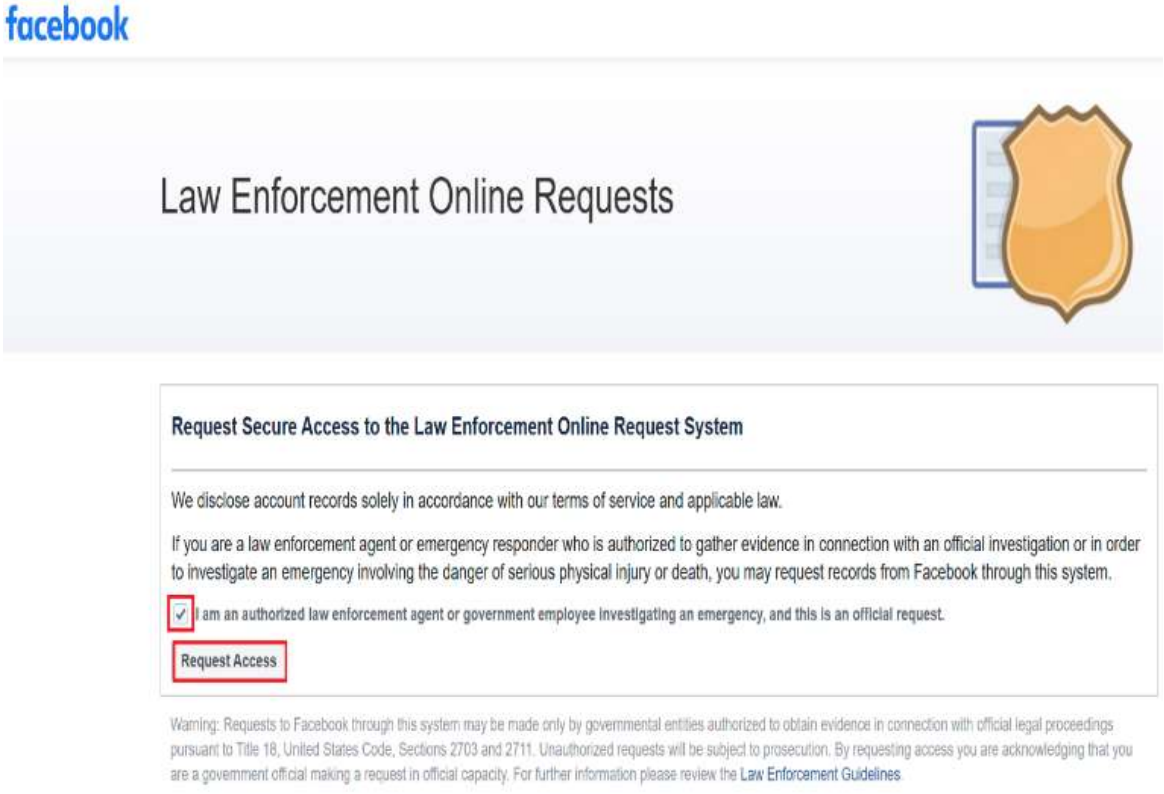
10. **Rule 7 of the IT Rules, 2021 – Non-observance of Rules**
    Where an intermediary fails to observe these rules, the provisions of sub-section (1) of section 79 of the IT Act shall not be applicable to such intermediary, and the intermediary shall be liable for punishment under any law for the time being in force including the provisions of the Act and the Indian Penal Code.

Chapter 2- Meta Platforms, Inc

The process for data disclosure requests for Meta Platforms, Inc., which includes Facebook, Instagram, and Oculus, is via a portal called the 'Law Enforcement Online Requests' Portal. The IO can preserve data, remove content and record requests on this portal. The following steps are to be followed:

1. https://www.facebook.com/records/login/ is the URL for the Data Disclosure Request Portal, which can be used to submit requests for Facebook and Instagram by any IO. The web page is shown in Picture 2.1. This Platform is commonly referred to as LEOR (Law Enforcement Online Report).

Picture 2.1: Law Enforcement Online Requests Web Page

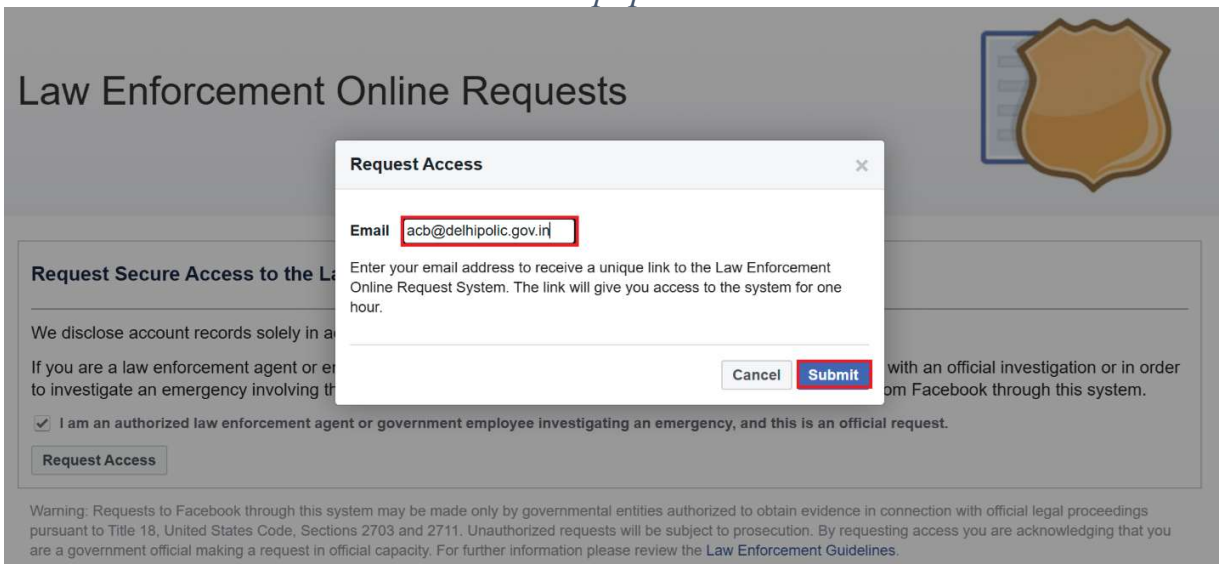


This web page provides secure access to Meta Platforms' Law Enforcement Online Request system to submit Record and Preservation requests. On this URL, the

concerned IO must submit an acknowledgement by clicking a check box that he is an authorised IO to submit an official request.

2. After ticking the checkbox, the concerned IO visits the portal by clicking on the "Request access" button on the web page. A popup window (Picture 2.2 below) will appear in which the IO needs to submit their Official Email ID.

Picture 2.2: Popup Window



3. After submitting the email ID, the concerned IO will get a link from Meta by email ID records@records.facebook.com, which will provide him with access to the LEOR Platform.

   If the IO is submitting the request for the first time, then he will get a link for a registration form. However, if the IO has submitted the request previously, he will be directly taken to the Requests dashboard shown in Picture 2.4

Registration

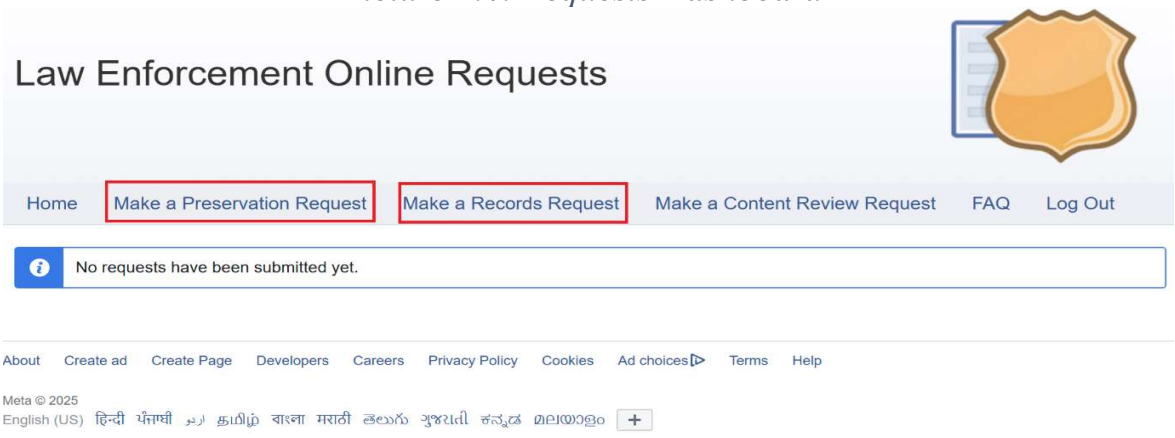
4. To register, the IO has to submit their details, i.e. Email, Name, Title, Organisation, Phone Number, Location and Postal code, as shown in Picture 2.3 on the next web page

Picture 2.3: Registration Web Page



5. After Submitting the request, the IO will be redirected to LEOR Platform Web page as shown in Picture 2.4

Picture 2.4: Requests Dashboard



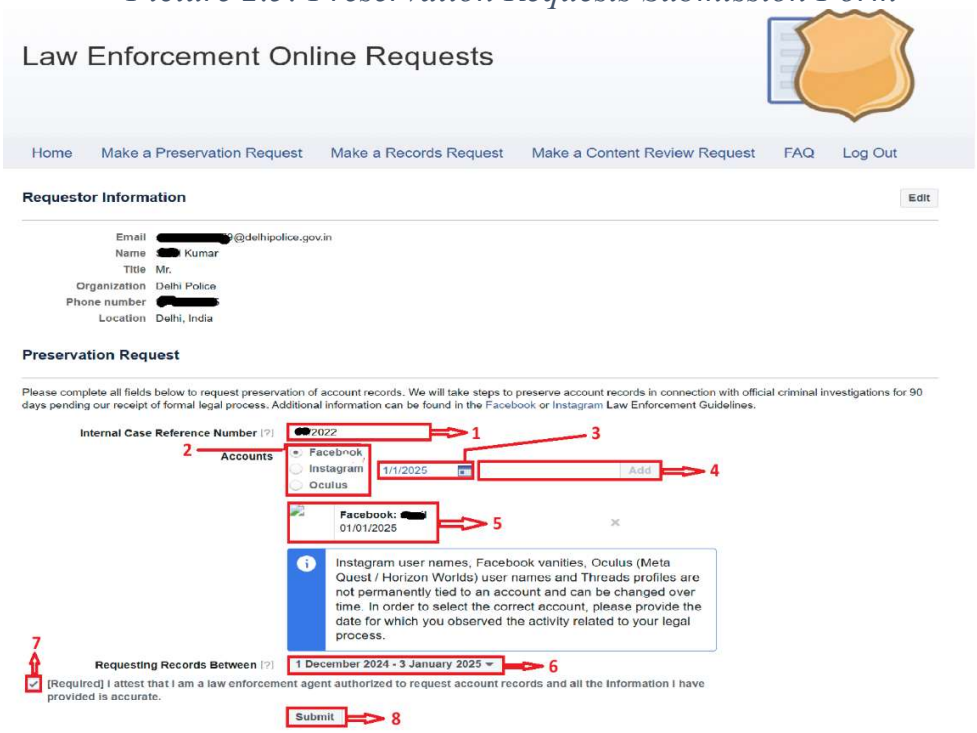
6. On this Web Page (Dashboard), the IO can make a request as per their requirements, like a Record Request or Preservation Request.

Preservation Request: If the IO wants Meta to preserve records like registration details or log details for future reference related to any Meta Users on Facebook or Instagram, they may submit a preservation request.

To Make a Preservation Request

When the IO Clicks on "Make a Preservation Request" on the request dashboard on the Requests web page (shown in Picture 2.4 above), a new web page will open, as shown in Picture 2.5 below

Picture 2.5: Preservation Requests Submission Form



The IO needs to submit the following details to submit a preservation request:

Field 1: **Internal Case Reference No**: refers to Complaint No./FIR No. or any other reference number.

Field 2: **Accounts**: Here, the platform on which the alleged account is operational needs to be selected.

Field 3: **Date**: Date on which the alleged account/profile was indulged in criminal activity

Field 4: Submit **the URL of the alleged account/profile** and Press the add button. IO may submit requests for multiple accounts/profiles here by adding them.

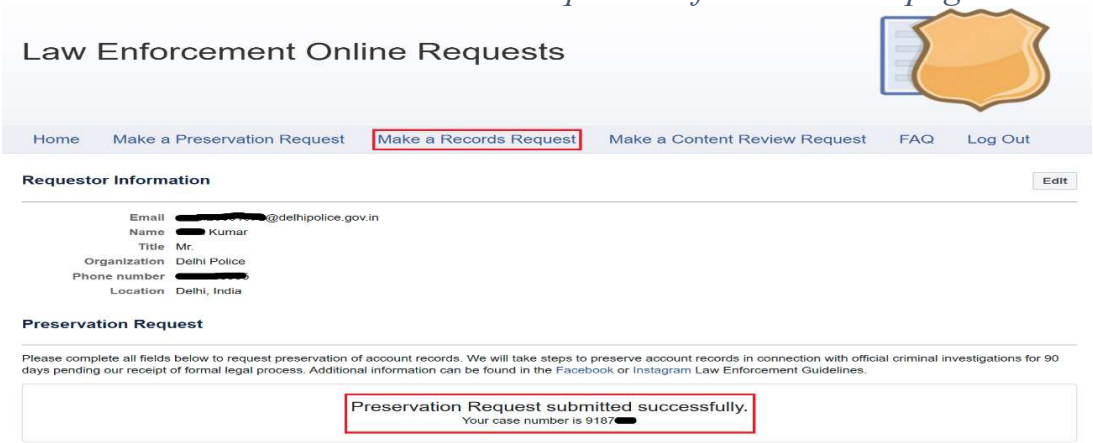
Field 5: After adding the details, the alleged submitted accounts/profiles, along with submitted dates, will be reflected in the next row.

Field 6: **Requesting Records Between**: In this field, the IO can submit the duration for which the details need to be preserved. It may be the period of alleged activities.

Field 7: **Check Box**: By clicking this checkbox, the IO acknowledges that they are an authorised officer and that all the information they have submitted is accurate.

Then the IO presses the 'Submit' button, and a preservation request will be submitted, and a case number will be generated (Picture 2.6). The IO must preserve it for future reference. This Case No. needs to be mentioned in every correspondence.

Picture 2.6: Preservation request confirmation web page



To Make Record Requests

Record Request: This option can be used by the IO to obtain details of the alleged account/profile, mobile number, IP logs, etc.

Picture 2.7: Record Request Submission Form



When IO Clicks on “Make a Records Request” (shown in picture 2.4), a new Web Page will open, as shown in Picture 2.7 above.

IO needs to submit the following details to submit a record request.

Field 9: **Internal Case No** refers to Complaint No. / FIR No. or any other reference number.

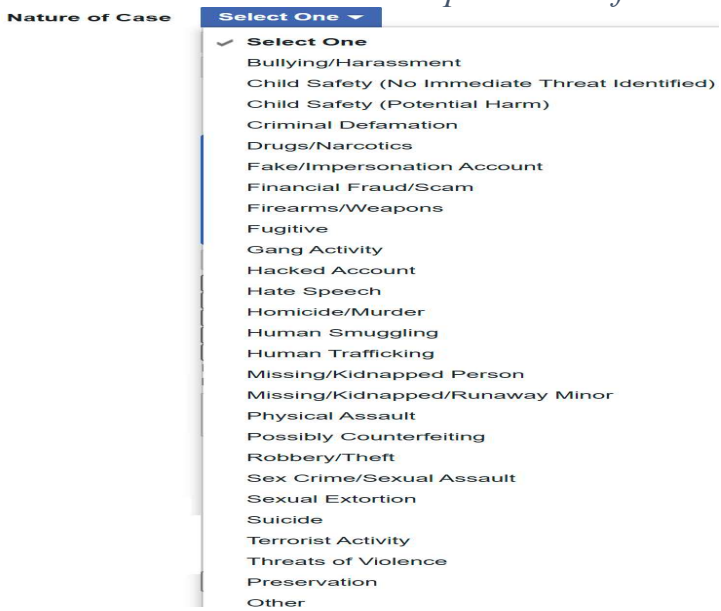
Field 10: **Legal Process**: In this dropdown menu, a list of sections is provided (Picture 2.8 below). In this, the IO needs to select the section/Type of Notice he/she is issuing to Meta, e.g. Section 91, 94 or Emergency, in case of any life threat.

Picture 2.8: Dropdown Menu for Legal Process



Field 11: **Nature of Case**: This dropdown menu provides a list of types of cases (Picture 2.9 below). The IO must select one based on the nature of the crime to which he is submitting the request.

Picture 2.9: Dropdown List for Nature of Case



Field 12: **Legal Process Signed Date**: In this option, the IO selects the date when the request letter is signed by the IO /Competent Authority.

Field 13: **Request Due Date**: In this option, the IO selects the date before which he wants to get records from Meta.

Field 14: **Accounts**: Here, the platform on which the alleged account (Facebook/Instagram) is operational needs to be selected.

Field 15: **Date**: Date on which the alleged account/profile was indulged in criminal activity and URL of the alleged account/profile and Press add button. IO may submit requests for multiple accounts/profiles here by adding them one by one.

Field 16: After adding the details, the submitted **alleged accounts/profiles**, along with submitted dates, will be reflected in the next row.

Field 17: **Requesting Records between**: In this field, IO submits the duration for which the details need to be obtained from Meta. It may be the period of alleged activities.

Field 18: **Documentation**: The IO must attach the signed letter/notice in pdf format in the 'documentation' section. The signed letter/notice shall be addressed to **Meta Platforms, Inc., 1 Meta Way, Menlo Park, CA 94025, United States of America.**

Field 19: **Additional Context**: The IO fills the Additional Context by providing sufficient information about the case, which is linked with the alleged profile/account.

Field 20: **Checkbox**: By clicking this checkbox, the IO acknowledges that he is an authorised Officer and that all the information he has submitted is accurate.

Then, the IO can press the '**Submit**' button, and a record request will be submitted, and a case no. will be generated (Picture 2.10). The IO must preserve it for future reference. This Case number needs to be mentioned in every correspondence.

Picture 2.10: Preservation Request Confirmation Web Page

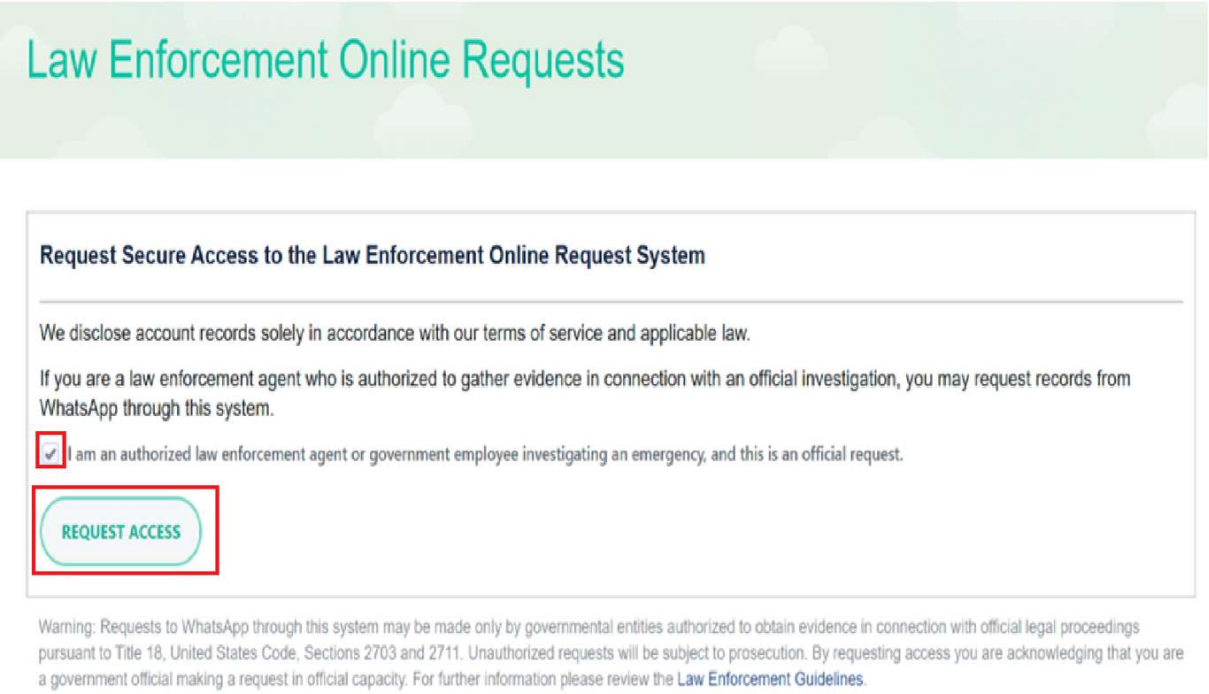


Chapter 3- WhatsApp LLC.

The process for data disclosure requests for WhatsApp, LLC is via a 'Law Enforcement Online Requests' portal, which is very similar to that of Meta Platforms, Inc. The IO can preserve data, remove content, and record requests on this portal. The following steps are to be followed:

1. https://www.whatsapp.com/records/login/ is the URL of WhatsApp LLC Data Disclosure Requests Portal. The web page is shown in Picture 3.1. This platform is commonly referred to as LEOR (Law Enforcement Online Report).

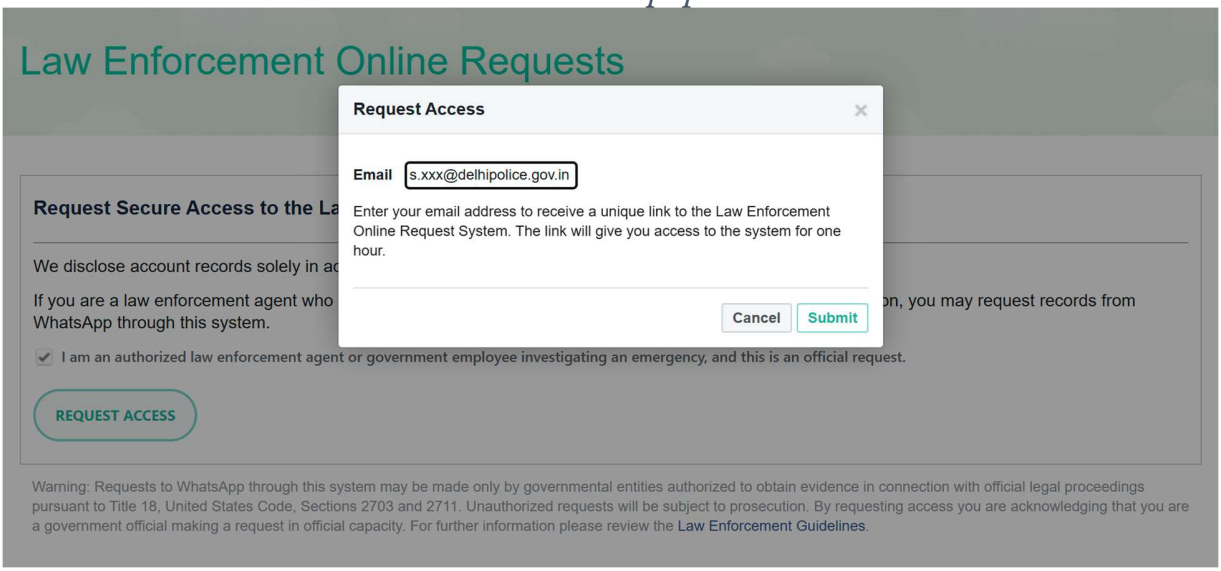
Picture 3.1: Law Enforcement Online Request Web Page



This web page provides secure access to the WhatsApp Law Enforcement Online Request system to submit Record and Preservation requests. On this URL, the concerned IO must submit an acknowledgement by clicking a check box that he is an authorised IO to submit an official request.

2. After ticking the checkbox, the Concerned IO visits the portal by clicking the "Request access" button on the web page. A popup window (as shown in Picture 3.2 below) will appear in which the IO needs to submit their Official email ID.

Picture 3.2: Popup Window



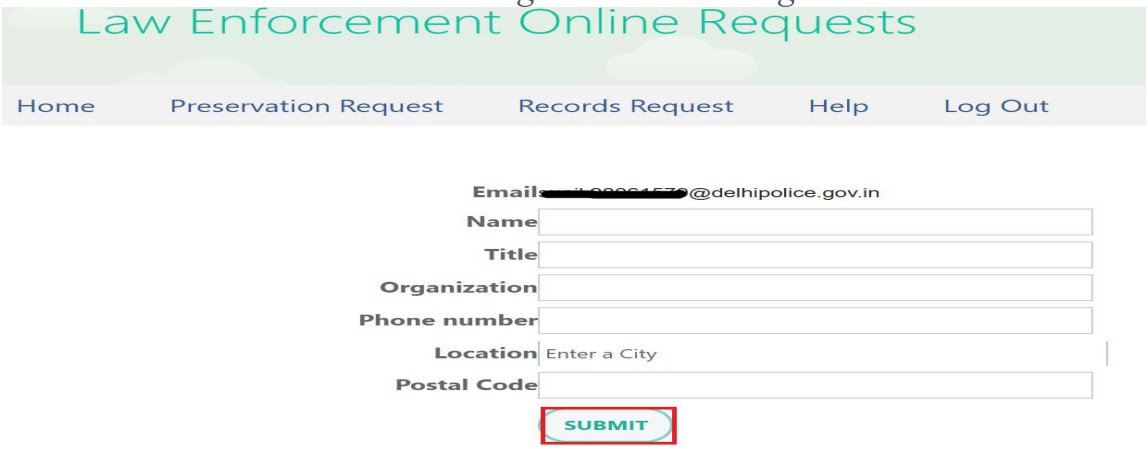
3. After submitting the email ID, the concerned IO will get a Link from WhatsApp Meta by email ID records@records.whatsapp.com, which will provide him with access to the LEOR Platform.

   If the IO is submitting the request for the first time, then he will get a link for a registration form. However, if the IO has submitted the request previously, he will be directly taken to the Requests dashboard shown in Picture 3.4

Registration

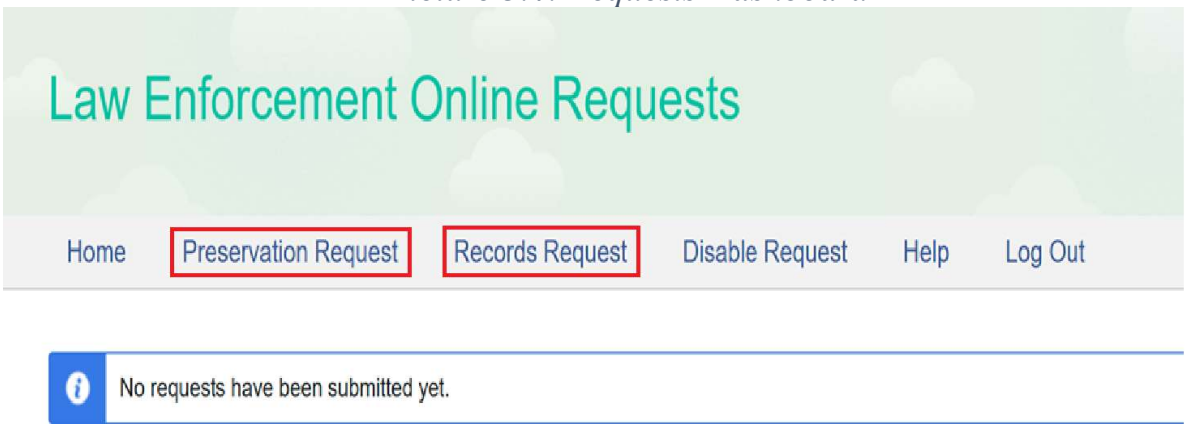
4. To register, the IO has to submit their details, i.e. Email, Name, Title, Organization, Phone Number, Location and Postal code, as shown in Picture 3.3 on the following web page.

Picture 3.3: Registration Web Page



5. After Submitting the request, the IO will be redirected to LEOR Platform Web page as shown in Picture 3.4

Picture 3.4: Requests Dashboard



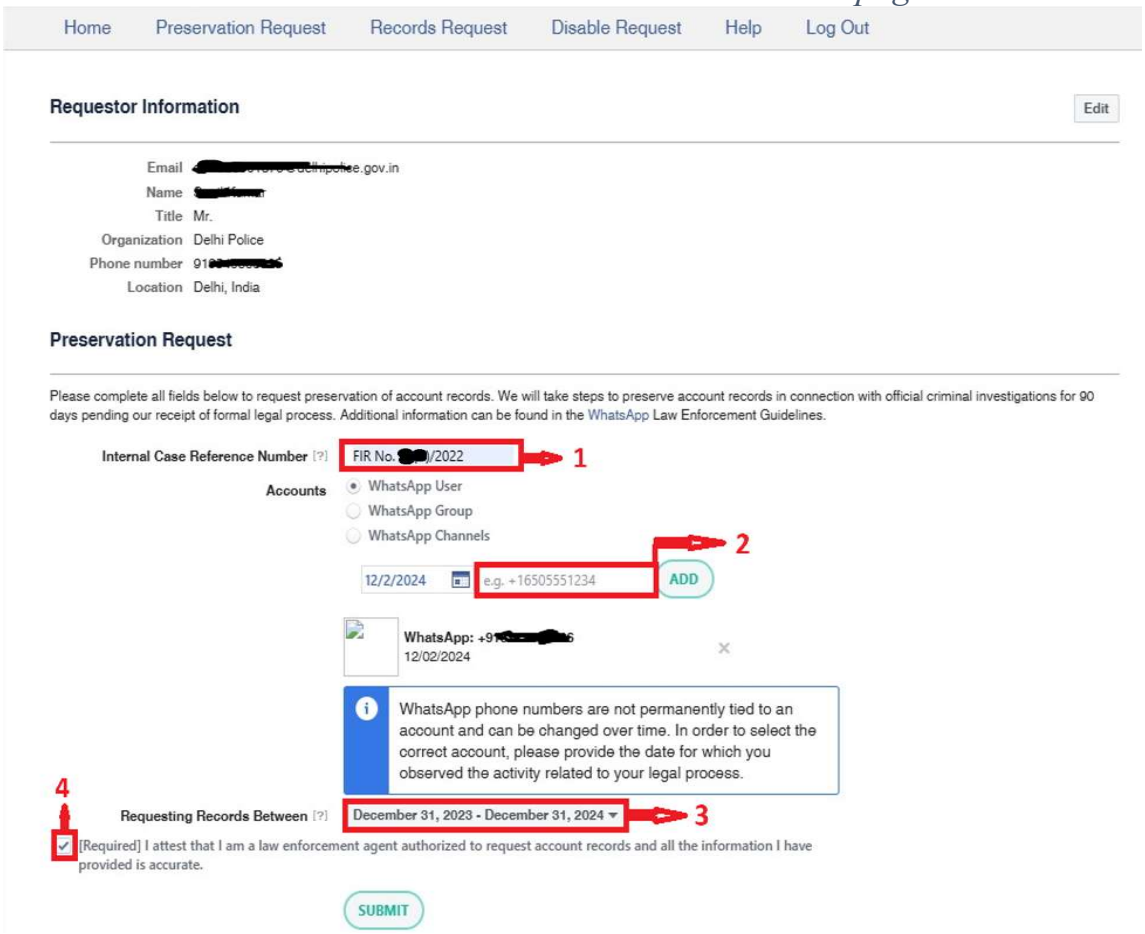
6. On this Web Page (Dashboard), IO can make a request as per his requirements, like Record Request or Preservation Request.

Preservation Request: If the IO wants WhatsApp, LLC to preserve records like registration details or log details for future reference related to any WhatsApp Users, then he may submit a preservation request.

To Make a Preservation Request

When IO Clicks on "Make a Preservation Request" on the request dashboard on the Requests Web Page (shown in Picture 3.4 above), a new Web Page will open, as shown in Picture 3.5 below

Picture 3.5: Preservation Submission web page



The IO needs to submit the following details to submit a preservation request:

Field 1: **Internal Case Reference No.** refers to Complaint No. / FIR No. or any other reference number.

Field 2: **WhatsApp number** by prefixing the country code, i.e. +91, for India mobile number and the date on which this WhatsApp number was indulged in criminal activity. The IO may submit requests for multiple

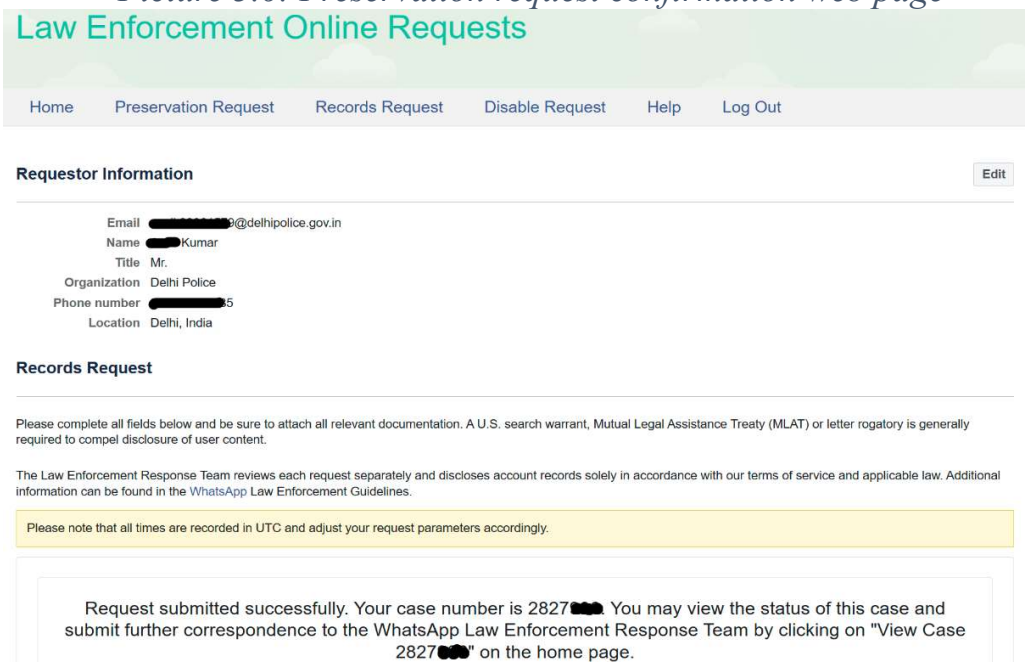
accounts/mobile numbers by adding them one by one. After adding the details, the alleged accounts/phone numbers that are submitted, along with the submitted dates, will be reflected in the next row.

Field 3: **Requesting Records Between**: In this field, the IO can submit the duration for which the details need to be preserved. It may be the date of alleged activities on which the alleged account/profile was indulged in criminal activity.

Field 4: **Check Box**: By clicking this checkbox, the IO acknowledges that he is an authorised officer and that all the information he has submitted is accurate.

Then, the IO press the 'Submit' button, and a preservation request will be submitted, and a case number will be generated (Picture - 3.6). The IO must preserve it for future reference. This Case No. needs to be mentioned in every correspondence.

Picture 3.6: Preservation request confirmation web page

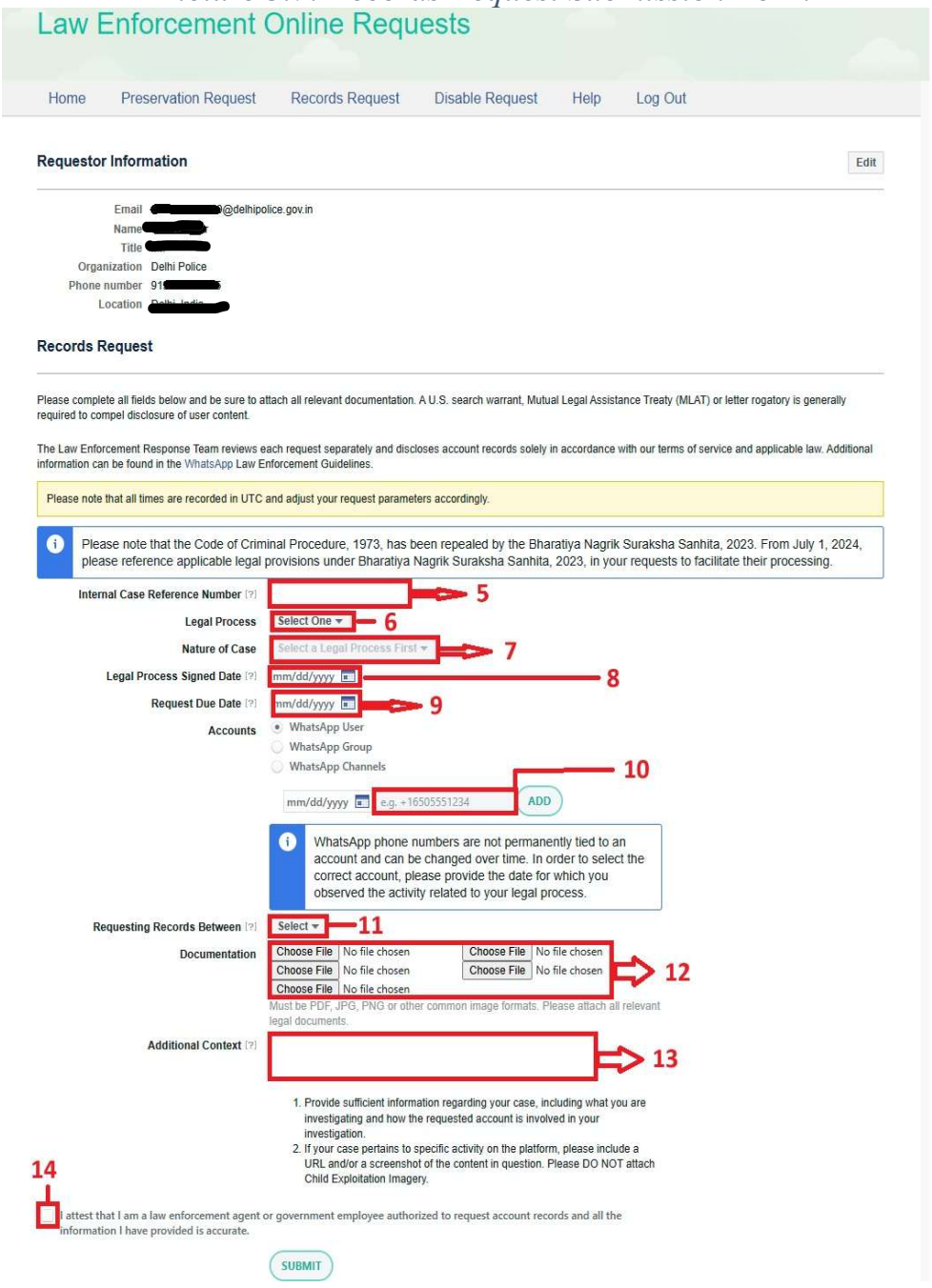


Record Request: This option can be used by the IO to obtain details of the alleged account/profile, Mobile No, IP Logs, group details, etc

To Make a Records Request

When IO Clicks on "Records Request" (shown in Picture 3.4 above), a new Web Page will open, as shown in Picture 3.7

Picture 3.7: Records Request Submission Form



The IO needs to submit the following details to submit a record request:

Field 5: **Internal Case Reference No.:** refers to Complaint No. / FIR No. or any other reference number.

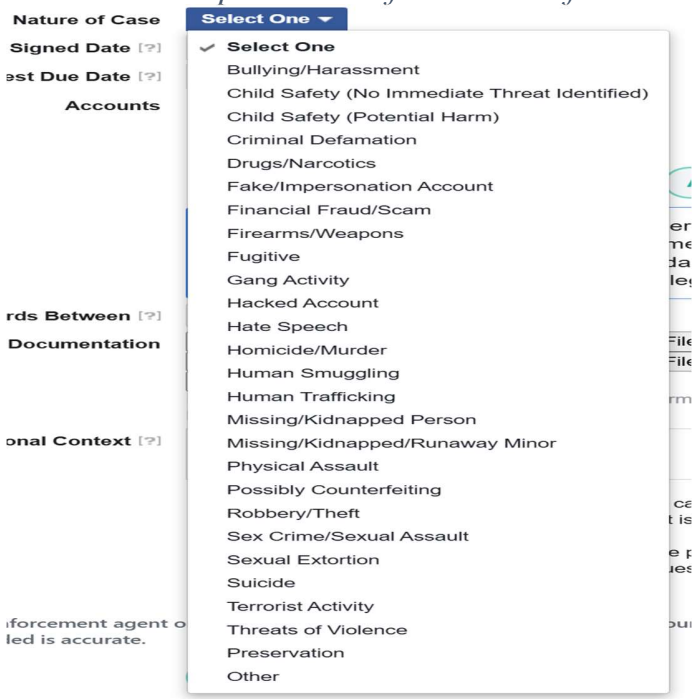
Field 6: **Legal Process**: In this dropdown menu, a list of sections (Picture 3.8) is provided for the IO to select the section/Type of Notice he/she is issuing to WhatsApp, e.g. Section 91 CrPC, 94 BNSS, etc.

Picture 3.8 Dropdown list for Legal Process



Field 7: **Nature of Case**: This dropdown menu provides a list of types of cases (Picture 3.9). The IO must select one based on the nature of the crime to which he is submitting the request.

Picture 3.8: Dropdown List for Nature of Case



Field 8: **Legal Process signed date**: In this option, the IO selects the date on which the notice/order of the IO / competent authority was signed.

Field 9: **Request Due Date**: In this option, the IO selects the date before which he wants to get records from WhatsApp.

Field 10: **Accounts**: In this section, the IO fills in the WhatsApp number by prefixing the country code, i.e. +91 for India mobile number and the date on which this WhatsApp number was indulged in criminal activity. The IO may submit requests for multiple accounts/mobile numbers by adding them one by one. After adding the details, the alleged submitted accounts/phone numbers, along with submitted dates, will be reflected in the next row.

Field 11: **Requesting Records Between**: In this field, the IO can submit the duration for which the details need to be taken. It may be the date of alleged activities on which the alleged account/profile was indulged in criminal activity.

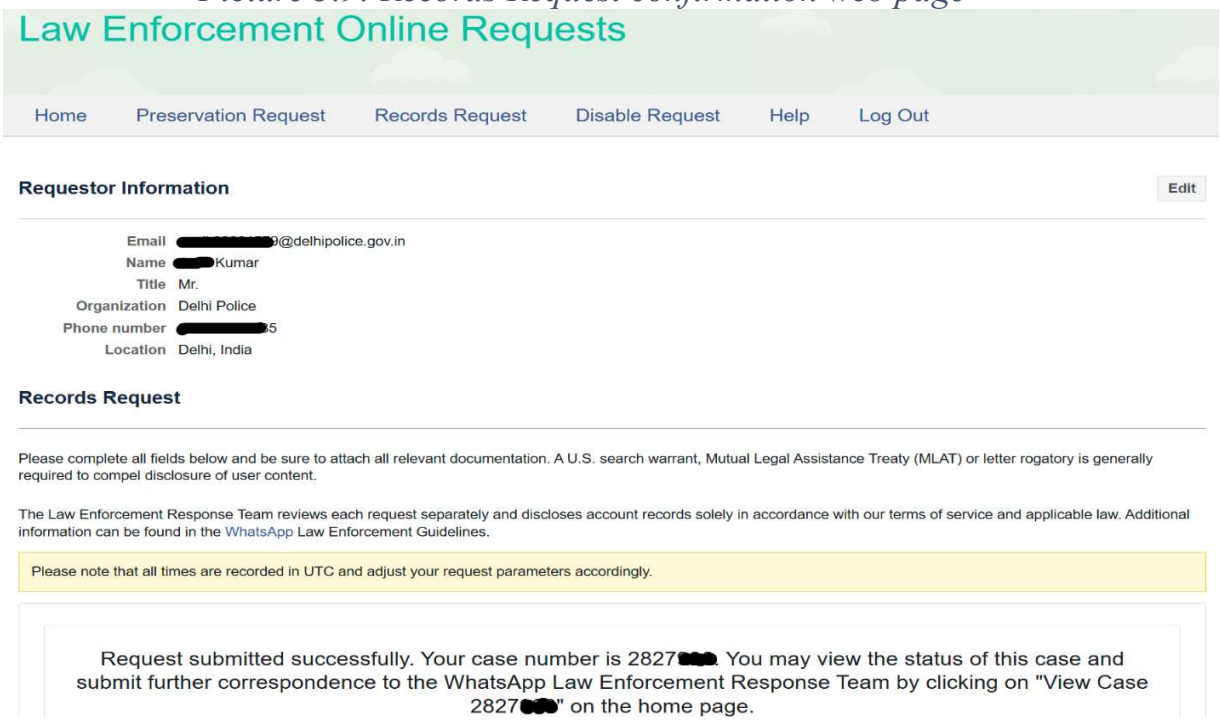
Field 12: **Documentation**: The IO must attach the signed letter/notice in pdf format in the 'Documentation' section. The signed letter/notice shall be addressed to **WhatsApp, LLC, 1 Meta Way, Menlo Park, CA 94025, United States of America**.

Field 13: **Additional Context**: The IO fills the Additional Context by providing sufficient information about the case, which is linked with the alleged profile/account.

Field 14: **Check Box**: By clicking this checkbox, IO acknowledges that he is an authorised Officer and that all the information he has submitted is accurate.

Then, the IO presses the 'Submit' button, and the record request is submitted, and a case number is generated (Picture 3.10). IO must preserve it for future reference. This Case number needs to be mentioned in every correspondence.

Picture 3.9: Records Request confirmation web page

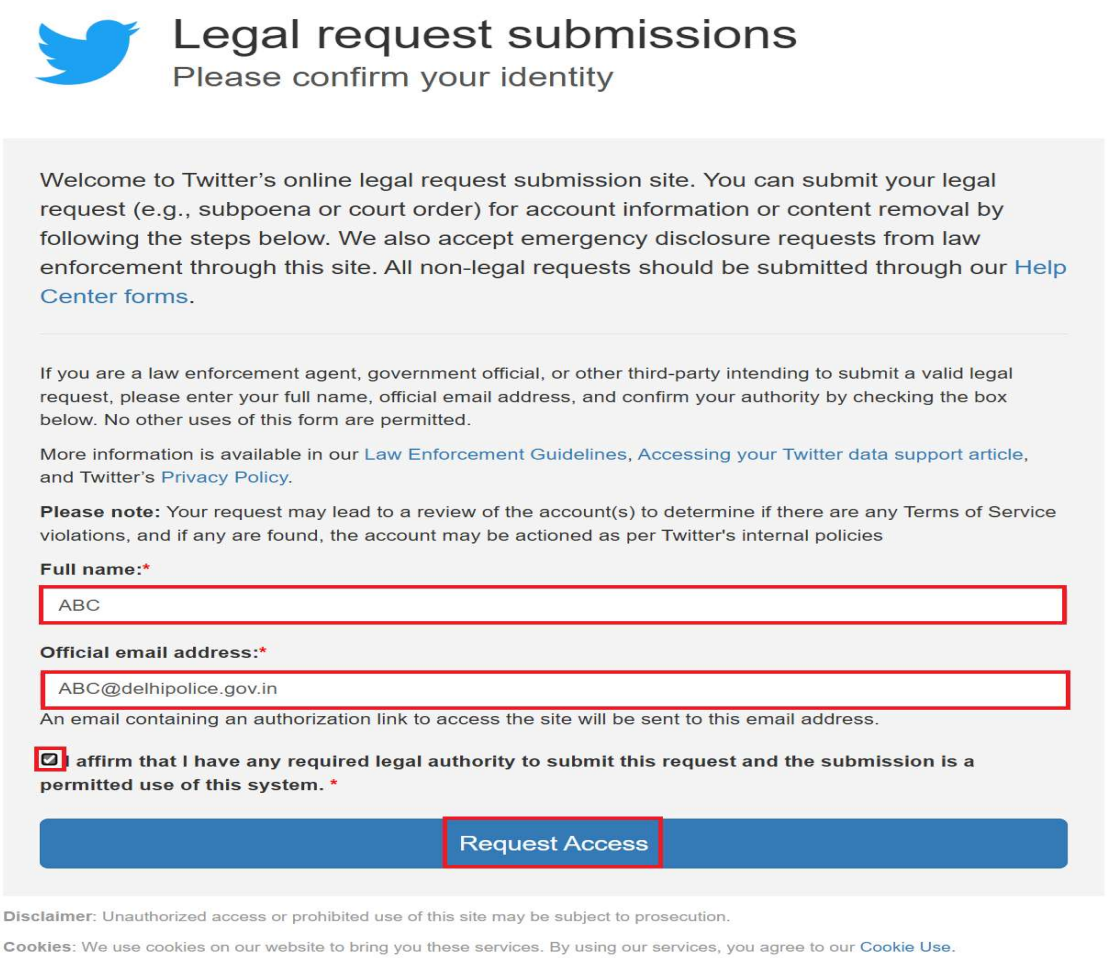


Chapter 4- X (Twitter) Corp.

X Corp., earlier known as Twitter, provides a "**Legal Request Submissions**" portal for police officers to submit data disclosure requests. This chapter lays down the process for data disclosure requests regarding X Corp. The following steps are to be followed:

1. https://legalrequests.twitter.com/ is the URL of X. that can be used to submit requests for X Corp. by an IO. The web page is shown in Picture 4.1.

Picture 4.1: Law Enforcement Requests Web Page

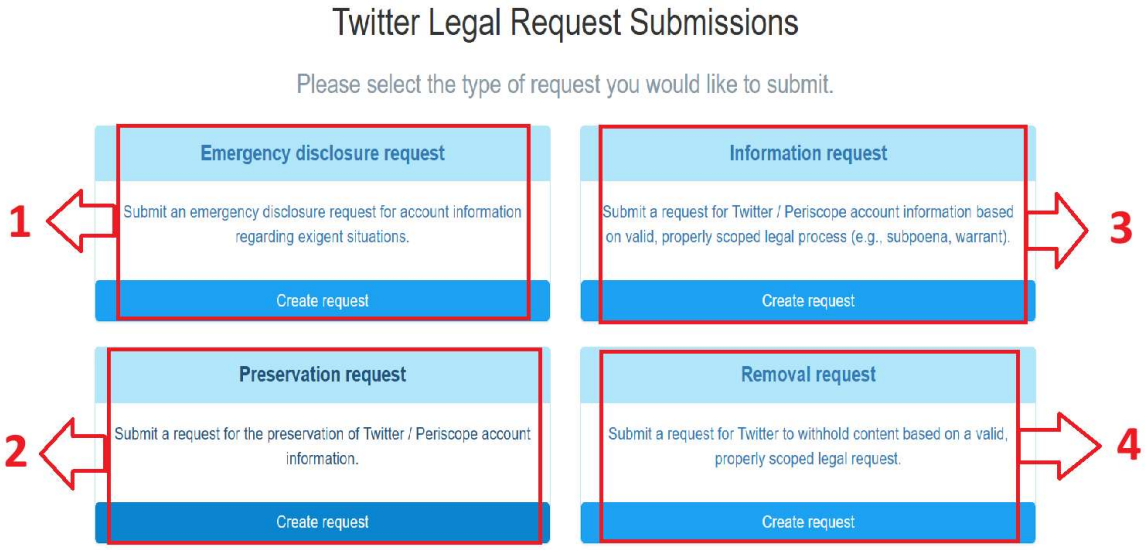


This web page provides secure access to X Legal Request Submissions to Submit Record and Preservation requests. On this URL, the concerned IO must submit an

acknowledgement by clicking a check box stating that he has required legal authority to submit the request and that the submission is a permitted use of this system.

2. After clicking the acknowledgement checkbox, the concerned IO visits the portal by clicking on the "Request Access" button provided on the Web Page
3. After submitting the name and email ID, the concerned IO will get a Link from X by email ID no-reply@twitter.com, which will provide him access to the Legal Requests Platform of X.
4. After clicking the "Request Access" button, a separate web page (Picture 4.2) will appear, on which the IO needs to submit their Official Email ID.

Picture 4.2: Requests Dashboard



5. On this page (Dashboard), the IO has four options to make requests as per their requirement, such as an emergency disclosure request, preservation request, information request, or removal request, as shown in Picture 4.2 above.

Emergency Disclosure Request: If the IO wants to make a data disclosure request in emergencies, he may submit an Emergency Disclosure Request. Emergencies, according to X Corp., are among the following entries (shown in Picture 4.3):

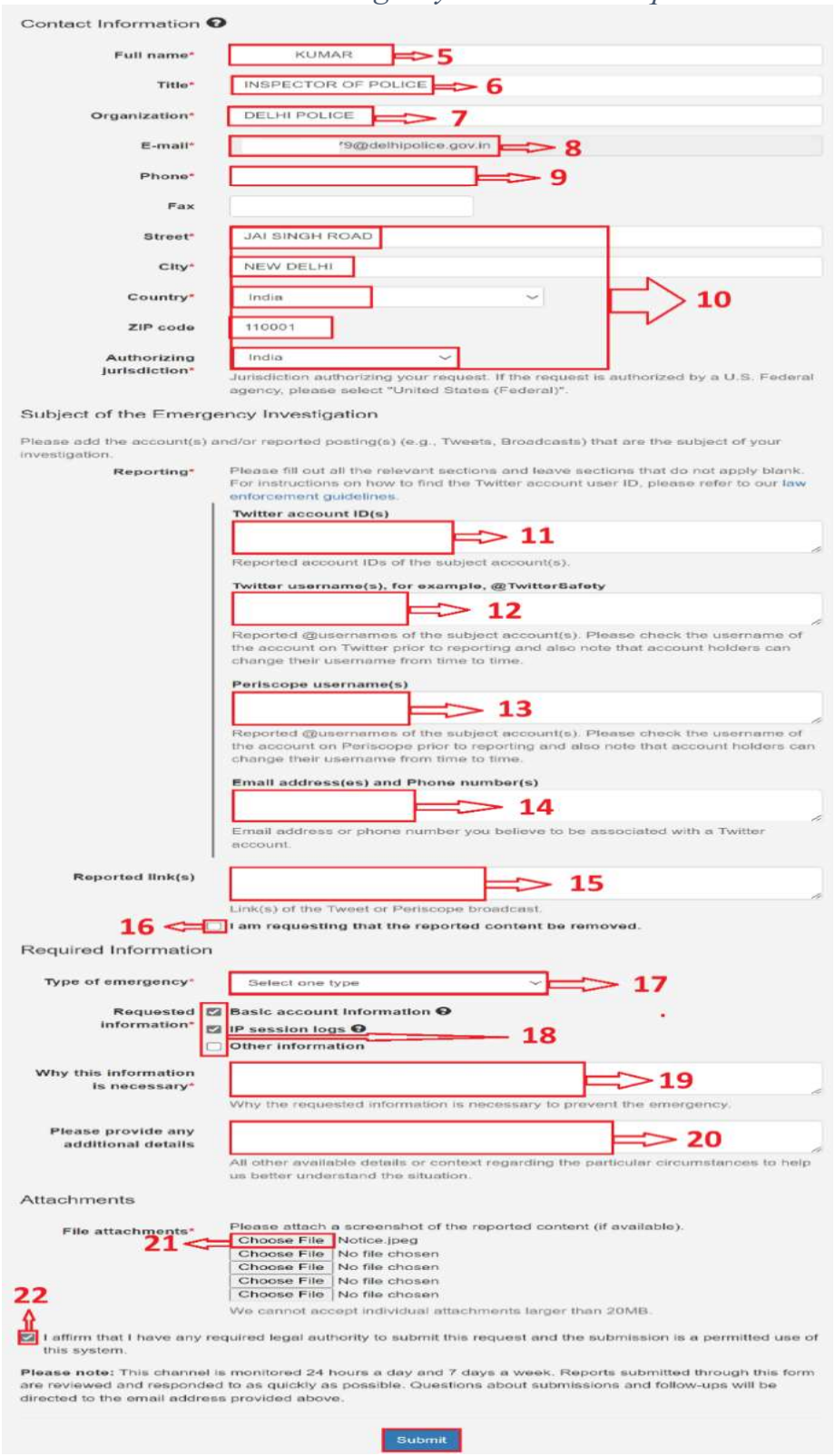
Picture 4.3: Emergency Situations List



To Make an Emergency Disclosure Request

When the IO clicks on 'Create Request' in Field 1, as shown in Picture 4.2, they will be redirected to X Emergency Disclosure Requests Web Page, as shown in Picture 4.4 below.

Picture 4.4: Emergency Disclosure Requests



The IO needs to submit the following details to submit a record request:

Field 5: **Name**: Full name of the IO.

Field 6: **Title:** Rank of the IO, i.e. Sub Insp., Insp. etc.

Field 7: **Organization**: Delhi Police.

Field 8: **Email**: Official email address of the IO making the request.

Field 9: **Phone**: Phone number of the IO making a request by prefixing the country code, i.e. +91.

Field 10: Official address of the IO.

Field 11: **Twitter Account ID:** the IO can enter the reported X account ID(s) (if available). If it is not available, this field may be left blank. However, it is advisable to provide Account IDs.

*Note: The account ID is the numerical ID of the user given by X Corp. It is unique to each user. e.g., the **Account ID of the Delhi Police X Account is 1850705408**, whereas the **username is DelhiPolice**, and the **Twitter Handle is @DelhiPolice**. The Account ID of any user is unique to any user and cannot be changed. However, the user can change the Twitter handle or username at a later stage.*

*To find the Account ID, one can use **https://findidfb.com/find-twitter-id/** and enter the username in the input textbox*

Field 12: **Twitter Usernames**: The IO fills up the X username(s). If it is not available, this field may be left blank.

Field 13: **Periscope Usernames**: the IO can enter the subject account's reported username(s) pertaining to Periscope (a video live streaming App). If it is not available, this field may be left blank.

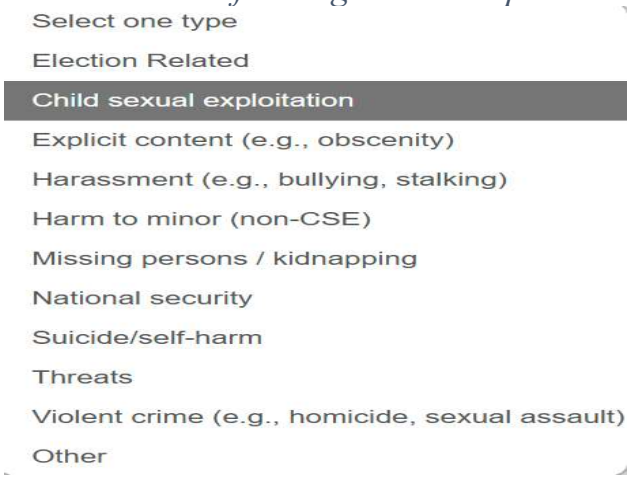
Field 14: **Email Addresses and Phone Numbers**: the IO fills up the mobile number(s) / email ID(s) associated with the subject account. If it is not available, this field may be left blank.

Field 15: **Reported Links**: Links of the required Tweet or Periscope broadcast

Field 16: **Check Box**: By clicking this checkbox, the IO can request the X even to remove the reported content from its web page.

Field 17: **Type of Emergency**: IO can select any of the emergencies from the dropdown menu, as shown in Picture 4.5 below.

Picture 4.5: List of Emergencies Dropdown Menu



Field 18: **Requested information**: Select the appropriate check boxes for basic account information, which includes the registrant details of the user, IP logs, or request any other information

Field 19: **Necessity**: The IO explains the necessity of the information to prove the emergency.

Field 20: **Additional Details**: The IO fills out the additional details of the case. If they do not have any additional information, it may be kept blank.

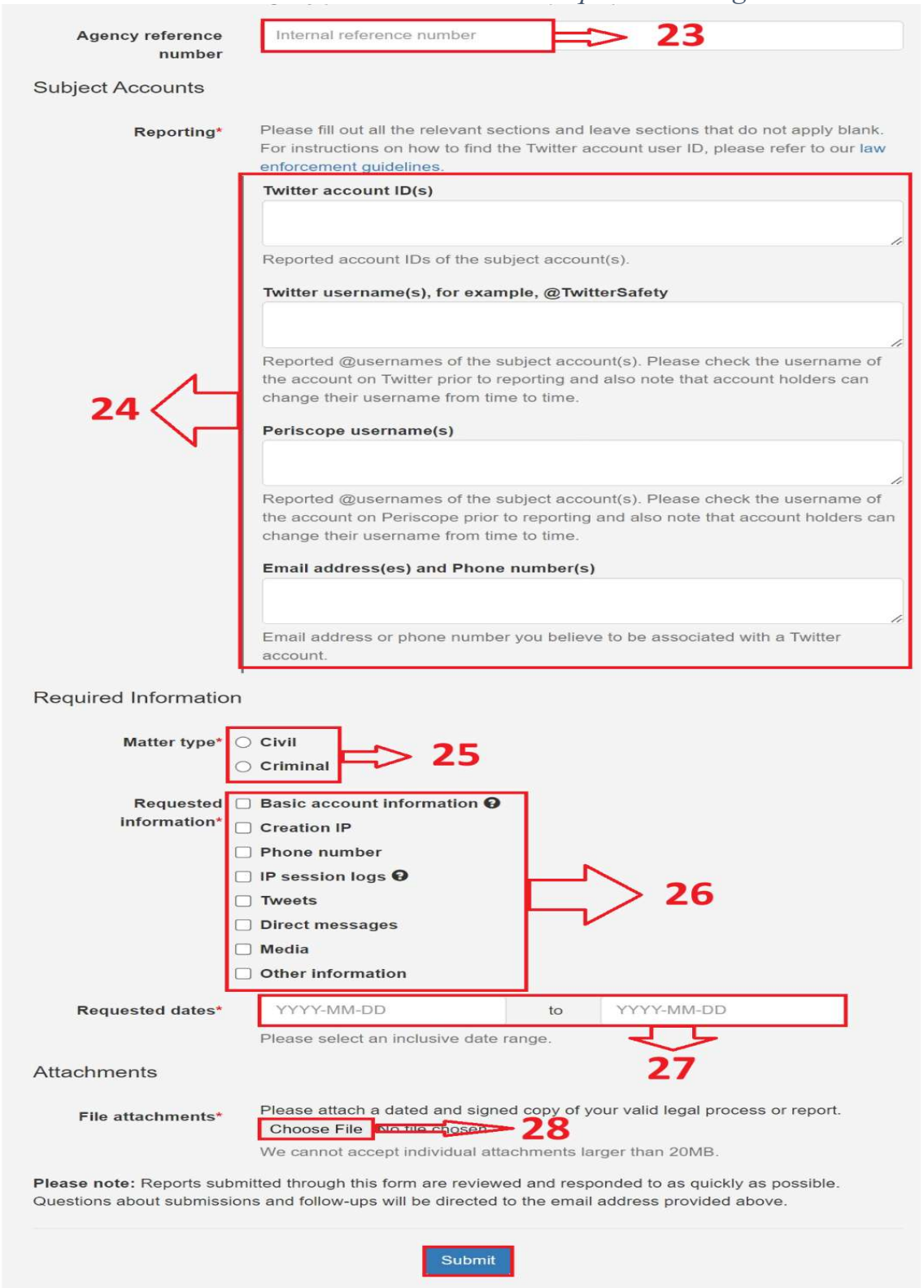
Field 21: In this field, the IO attaches the signed letter(s)/order(s) in pdf/jpg format. The attachment should not be larger than 5 MB in size.

Field 22: Check Box: By clicking this checkbox, the IO acknowledges that he is an authorised Officer and that all the information he has submitted is accurate. Upon clicking the submit button, the emergency request is submitted.

Preservation Request

If the IO wants to make a preservation request, then he may submit it by clicking on 'Create Request' in Field 2, as shown in Picture 4.2 Request Dashboard. The following web page (dashboard) is shown in Picture 4.6, will be opened.

Picture 4.6: Preservation Request Web Page



IO needs to submit the following details to submit a preservation request:

Field 23: **Agency Reference Number**: refers to Complaint No. / FIR No. or any other reference number.

Field 24: The IO can enter the X account ID(s) / username / Periscope username/email address(s) / phone number(s) as shown on the Emergency Disclosure Requests Web page. (Fields 11-14)). Unknown fields can be left blank.

Field 25: **Matter Type**: The IO will select the matter type, i.e., civil/criminal.

Field 26: **Requested Information**: The IO can select any of these checkboxes as per their requirement for the preservation of that information.

Field 27: **Requested Dates**: IO can submit the duration of which the details need to be taken. It may be the date of alleged activities on which the alleged account/profile was indulged in criminal activity.

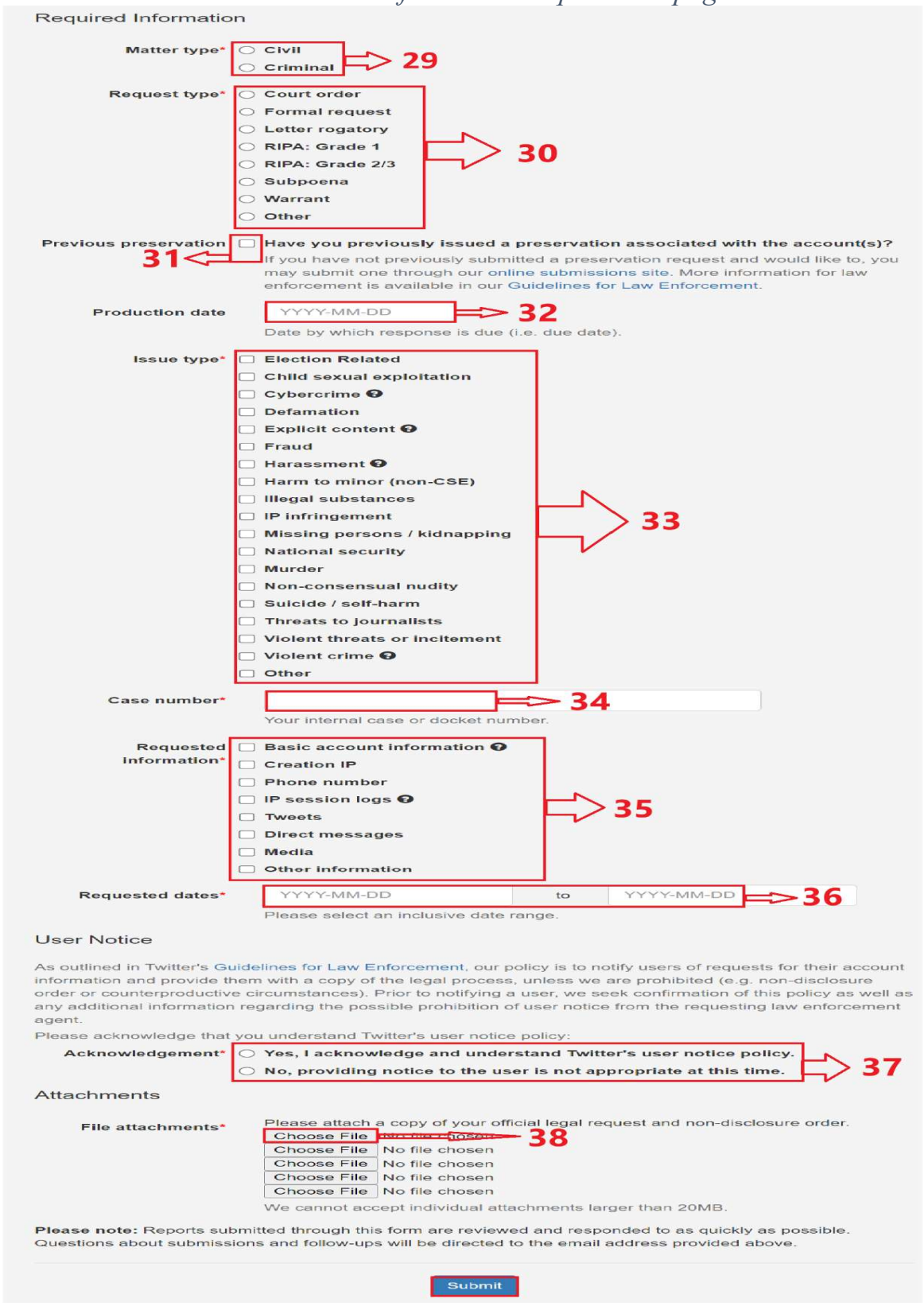
Field 28: **Attachment**: The IO must attach the signed letter or notice in pdf format in this section.

Upon clicking the submit button, the request is submitted.

Information Request

For ordinary data disclosure requests, the IO can click on Create Request in Field 3 on Picture 4.2: Requests Dashboard, they will be redirected to the X Legal Request Submission Web page, as shown in Picture 4.7.

Picture 4.7 Information Request web page



IO needs to submit the following details to submit an information request:

Field 29: **Matter Type**: the IO selects the appropriate option (civil/criminal).

Field 30: **Request Type**: The IO may select the appropriate options from court order, format request, Letter Rogatory, etc.

Field 31: **Previous Preservation**: Select this option if any previous preservation requests have been made. If no request has been made, it must be left blank.

Field 32: **Production Date**: The IO fills up the date on which they want to get information from X.

Field 33: **Issue Type**: The IO selects the nature of the crime of the case for which they are making a request from X for information.

Field 34: **Case Number:** The IO fills up the Internal Case No, i.e. Complaint No/FIR No. or any other reference number.

Field 35: **Requested Information:** In this field, the IO selects the options as per the requirements of their case. It is the information that the IO want to get from X. In this field, Basic account information includes the creation date, email address, and/or phone number on record, if available, can be requested.

Field 36: **Requested Dates:** In this field, the IO fills in the dates on which the alleged account/profile indulged in criminal activity and the URL of the alleged account/profile. IO may submit requests for multiple accounts/profiles in one request.

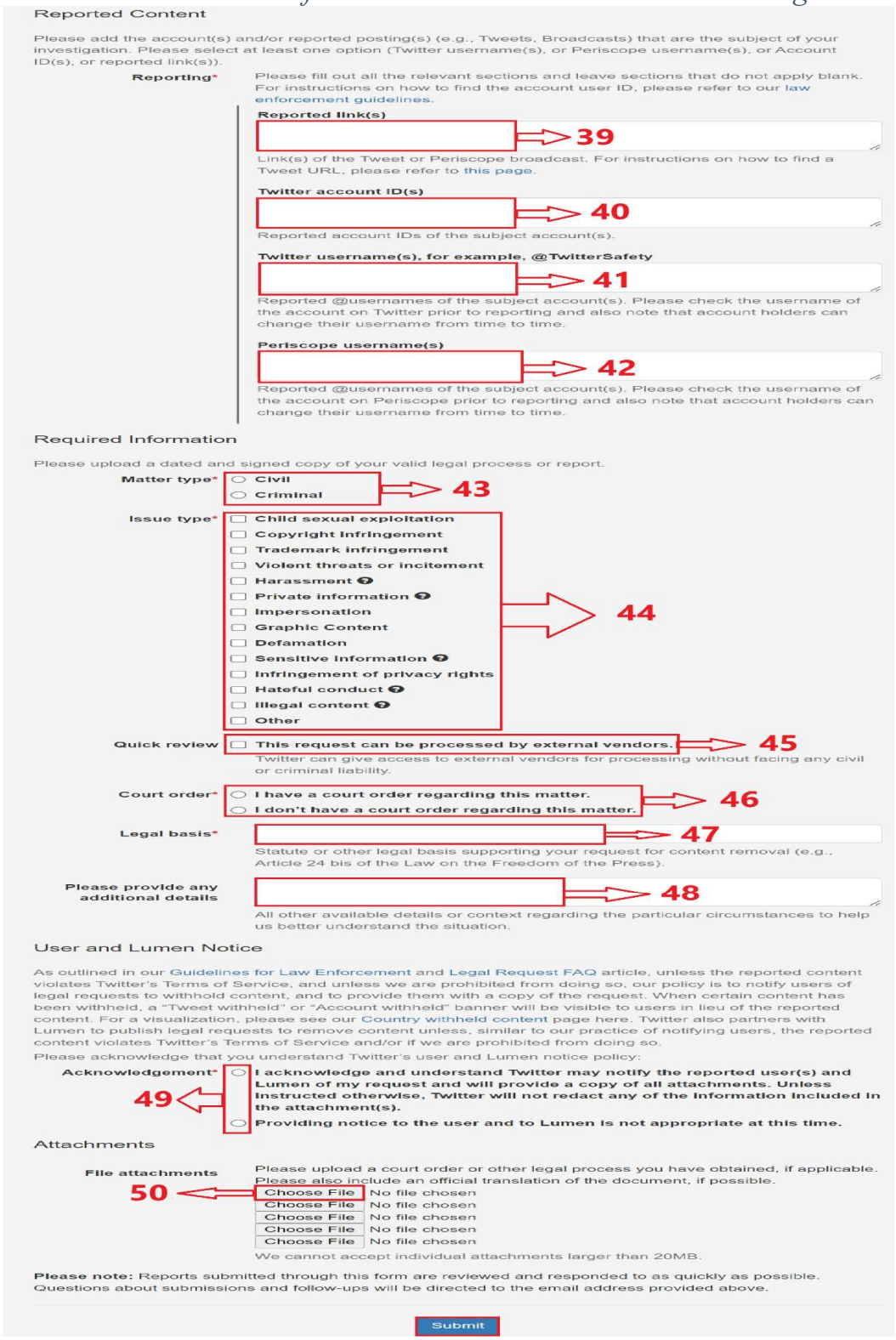
Field 37: **Acknowledgement:** In this field, the IO should mark 'No' if they want the X not to notify the user about the notice of the IO. **It is, as per X's policy, that the LEA notifies the users that the LEA is seeking information about the user.**

Field 38: **Attachment:** The IO must attach the signed letter/notice in pdf format in the 'documentation' section. After the attachment, the IO presses the submit button, and the request is submitted.

Removal Request

If the IO wants to submit a removal request, then he / she may do so by clicking on 'Create Request' in Field 4 as shown in Picture 4.2, and they will be redirected to X Information Removal Submission Web page as shown in Picture 4.8. IO needs to submit the following details to submit a removal request:

Picture 4.8: Information Removal Submission Web Page



Field 39: **Reported Link:** In this field, the IO fills up the reported link(s) of the subject account.

Field 40: **Twitter Account ID**: In this field, the IO fills up the X account ID(s) (if they have one). If it is not available with the IO, they may leave it blank.

Field 41: **Twitter username**: In this field, the IO fills up the username(s) of the subject reported account. If it is not available with the IO, they may leave it blank.

Field 42: **Periscope username**: In this field, the IO fills up the username(s) of the subject reported account pertaining to Periscope, a video live streaming App. If it is not available with the IO, they may leave it blank.

Field 43: **Matter Type**: In this field, the IO selects the matter type, i.e. civil/criminal.

Field 44: **Issue Type**: In this field, the IO selects the issue type/ nature of the crime of the case for which they are making a request from X for removal.

Field 45: **Quick Review**: If IO wants to get the reported content review quickly, then he marks it in the checkbox. The X may give external vendors access to the content for processing. It is the prerogative of the IO and he / she has to take decision based on facts and circumstances of the case/complaint.

Field 46: **Court Order**: In this field, the IO has to select the option, if the court order is available.

Field 47: **Legal Basis**: In this field, the IO fills the legal statute (section of law) on which base the removal request is being made from X.

Field 48: **Additional Details**: In this field, the IO fills up the additional details of the case. If he / she does not have any additional information, it may be kept blank.

Field 49: **Acknowledgement**: In this field, IO marks tick at 'Providing notice to the user and to Lumen is not appropriate at this time'. It is the policy of X that it notifies the users that the LEA is seeking information about him (user).

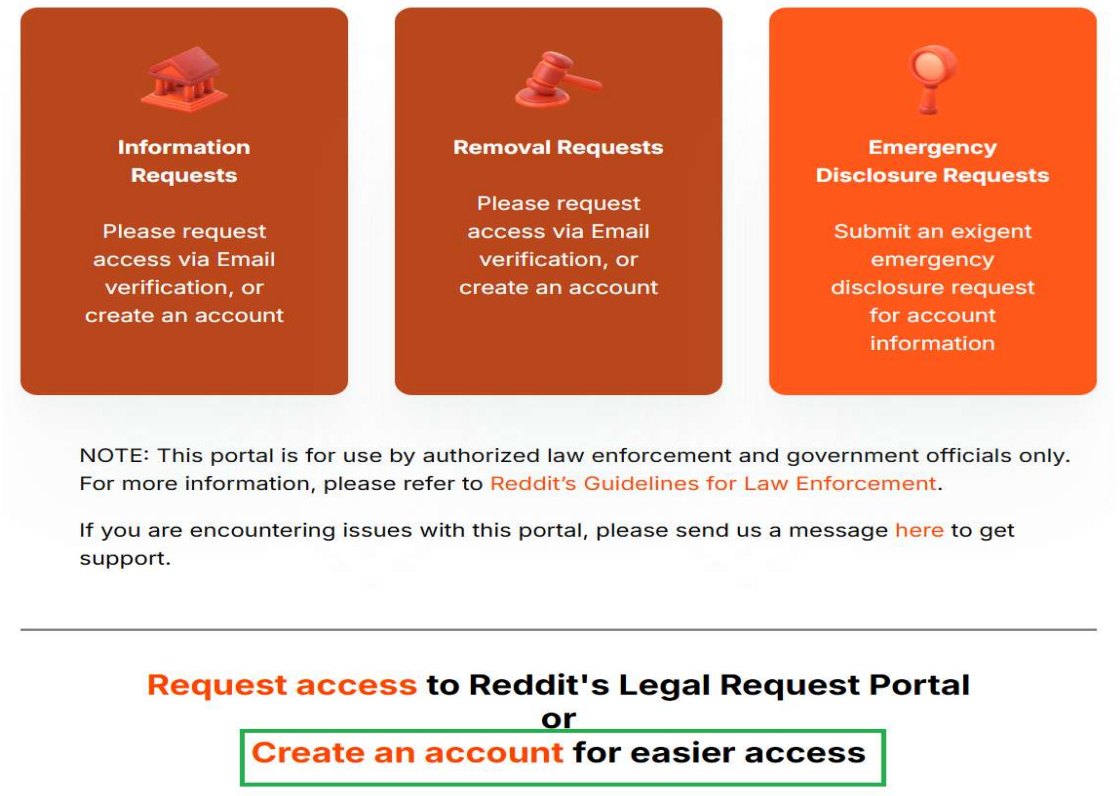
Field 50: **Attachment**: The IO must attach the signed letter/notice in pdf format in 'documentation' section. After attachment, the IO presses submit button and the request is submitted.

Chapter 5- Reddit, Inc.

Reddit, Inc., provides a "**Legal Requests**" portal for police officers to submit data disclosure requests. This chapter lays down the process for data disclosure requests regarding Reddit, Inc. The following steps are to be followed:

1. https://legalrequests.reddithelp.com/hc/en-us/requests/new is the URL that can be used to submit requests for Reddit, Inc. by any IO. The web page is shown in Picture 5.1 below.

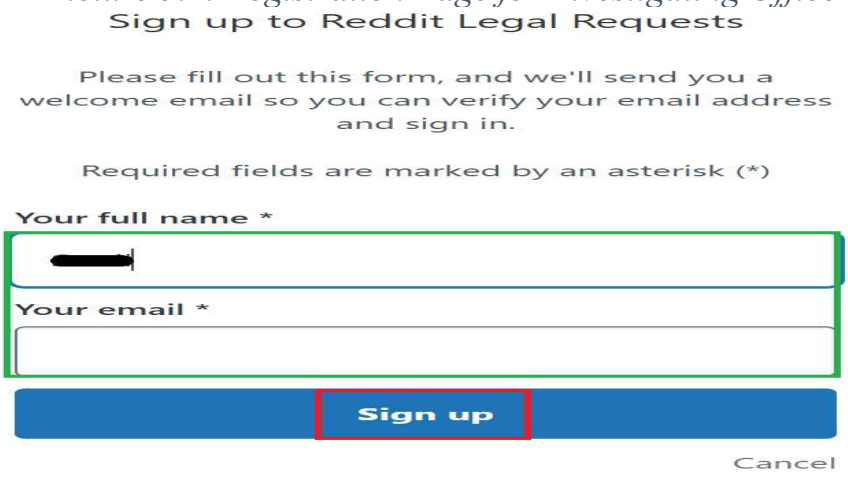
Picture 5.1: Law Enforcement Requests Access Web Page



This web page provides secure access to Reddit Legal Request Submissions to get Information, Removal and Emergency Disclosure requests. On this URL, IO must create an account by clicking at 'Create an account'.

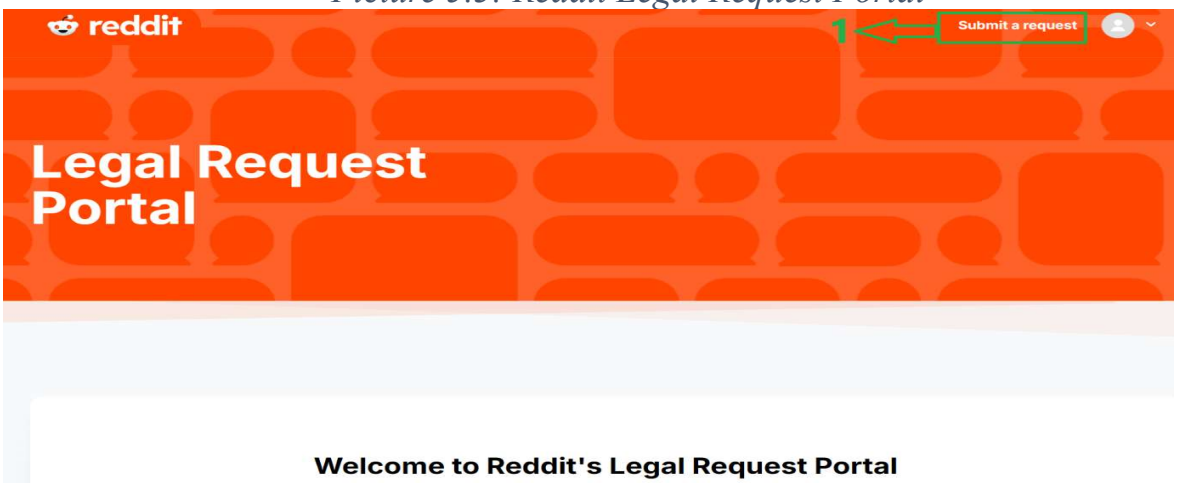
2. After clicking the ‘Create an account’, the concerned IO visits the portal and the Web Page shown in Picture 5.2 below opens.

Picture 5.2: Registration Page for Investigating Officer



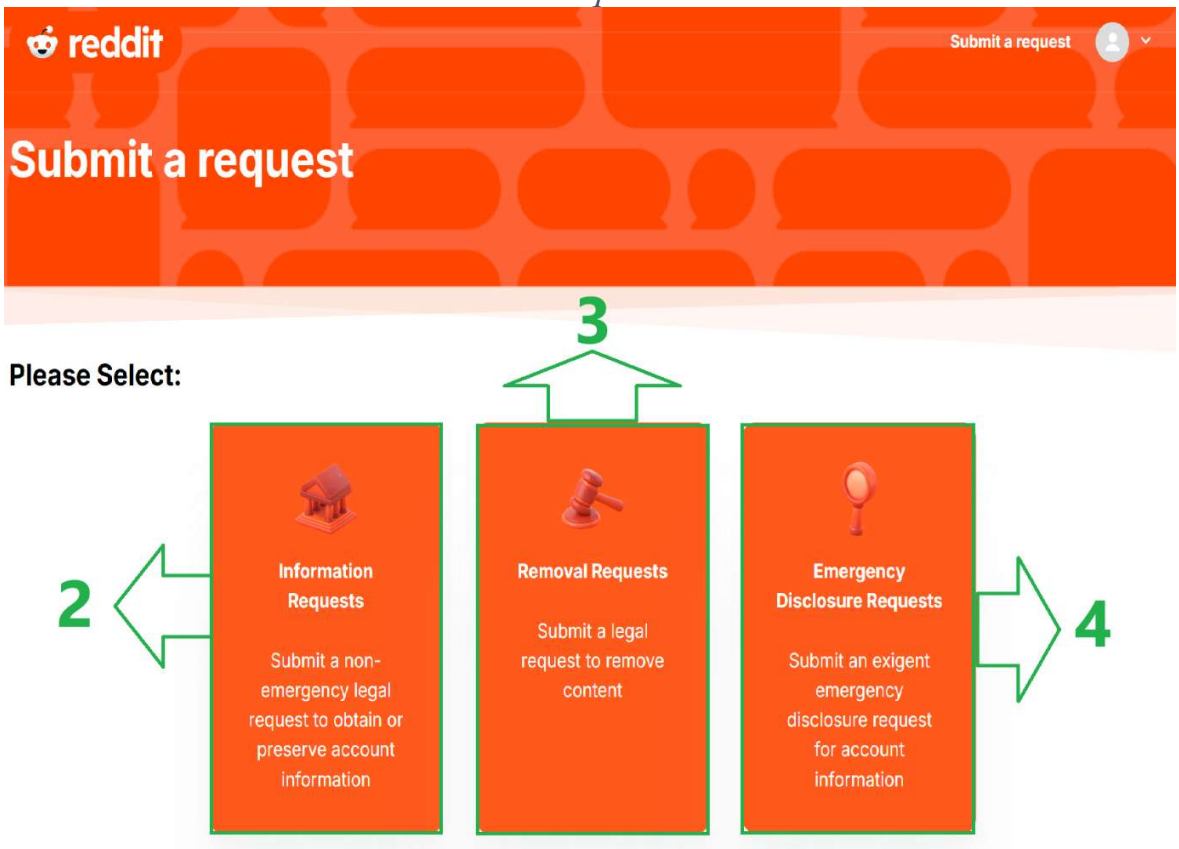
3. After Submitting the name and **official email ID**, the concerned IO will get a Link from Reddit by email ID support@reddit-plp.zendesk.com. The IO clicks the link to create a password and sign in. Thereafter the IO sign in the portal by inserting his login details and the web page shown in Picture 5.3 opens. The IO should click at ‘Submit a request’ button located on the top right corner of web page as shown in Field 1 in right corner of Picture 5.3

Picture 5.3: Reddit Legal Request Portal



On this page (Dashboard), the IO can make requests as per their requirements, such as information requests, removal requests or emergency disclosure requests, as shown in Picture 5.4.

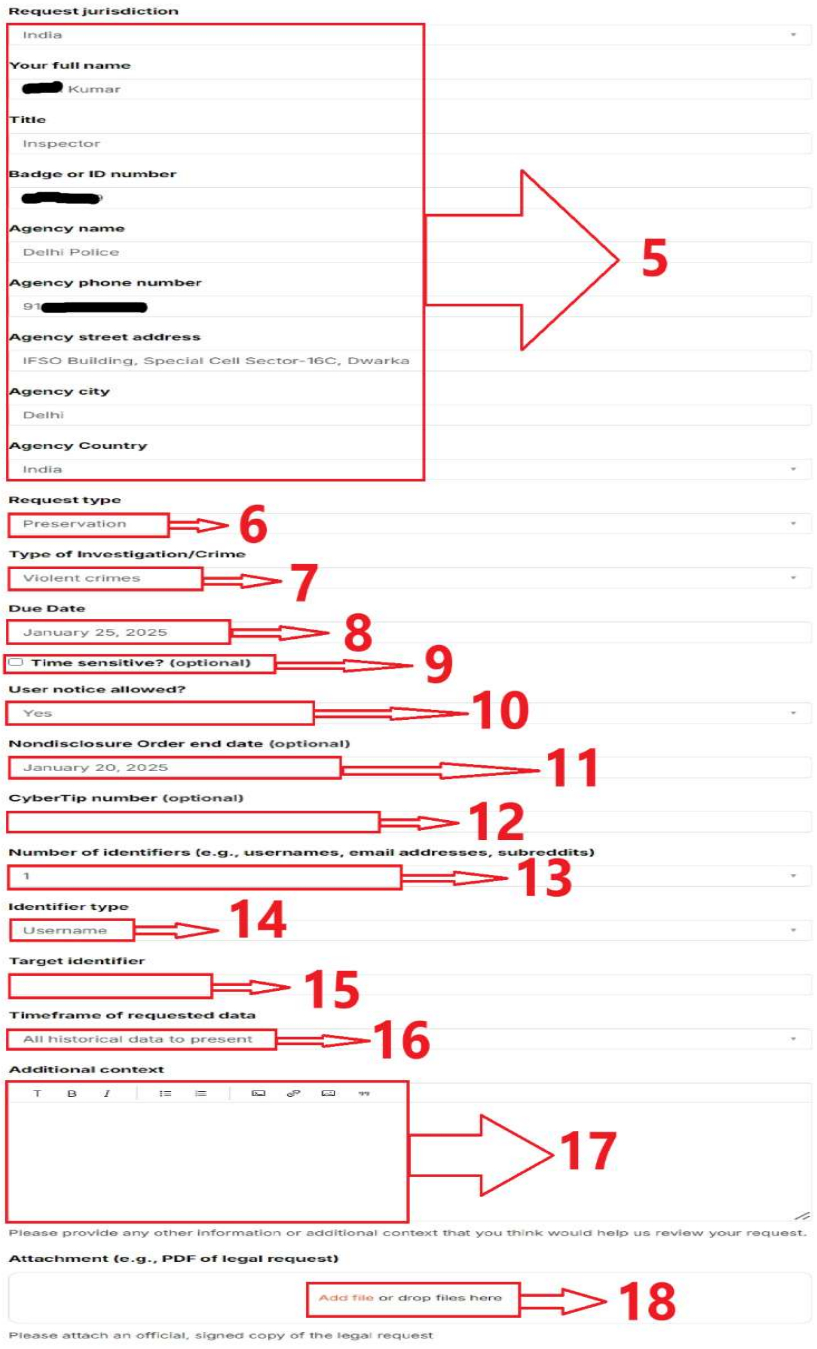
Picture 5.4: Requests Dashboard



Information request

If the IO wants to submit a non-emergency request for preservation or for data disclosure, then he may submit information request by clicking Information Request in Field 2, in Picture 5.4, and Picture 5.5 (Information Request submission web page) shall open.

Picture 5.5 Information Request Submission Web page



Field 5: **Basic Information of the IO:** Full name, title / Rank of the IO i.e. Sub Insp., Insp. etc., badge number i.e. PIS No. and phone number of the IO as well as other information related to Agency i.e. Delhi Police.

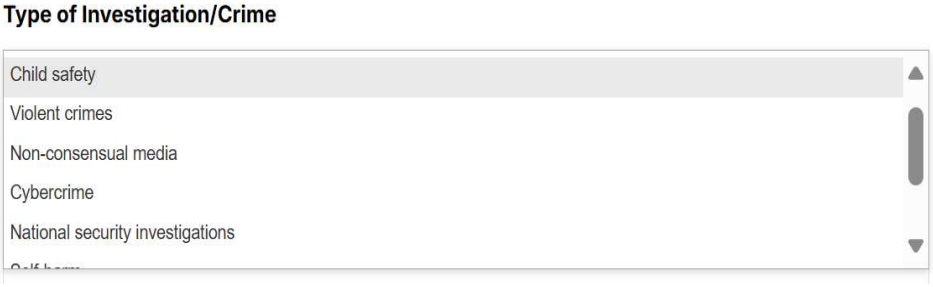
Field 6: **Request Type:** The IO selects the request type, i.e. preservation, court order, etc., from the dropdown as shown in Picture 5.6.

Picture 5.6 Request Type dropdown



Field 7: **Type of Investigation**: The IO select crime type from dropdown menu 'type of Investigation/Crime' as shown in Picture 5.7

Picture 5.7 Type of investigation/crime dropdown



Field 8: **Due date**: The IO selects the date when they want to get the information from Reddit.

Field 9: **Time Sensitive**: The IO ticks the checkbox if the information is time sensitive. It is optional, so he / she may leave it, if not required.

Field 10: **User notice allowed**: The IO should select 'no/yes'. If they select Yes, Reddit will notify the users that the LEA is seeking information about (the user). If no is selected, the Reddit won't notify the user.

Field 11: **Non-disclosure order**: If IO has any non-disclosure order from the Hon'ble court, then mention the date of the order. This is optional.

Field 12: **Cyber-tip number**: If IO has any tip reference number from any agency/freelancer/source, then it may be filled. This is, however, optional.

Field 13: **Number of Identifier**: In this field, the IO selects the number of identifiers (*identifier means user's unique details*) i.e. 1, 2, 3, etc. in their case about whom they want information from Reddit.

Field 14: **Identifier Type**: In this field, the IO selects an identifier, i.e. username, email, or other. (The username may be available in one case, and in another email, it might be available)

Field 15: **Target Identifier**: In this field, the IO fills in the details of the identifier, i.e. username, email ID, etc.

Field 16: **Timeframe**: In this field, the IO selects duration. They may give any particular duration, or they may seek all historical data of the user identifier.

Field 17: **Additional Information**: In this field, the IO fills in the additional information about the user.

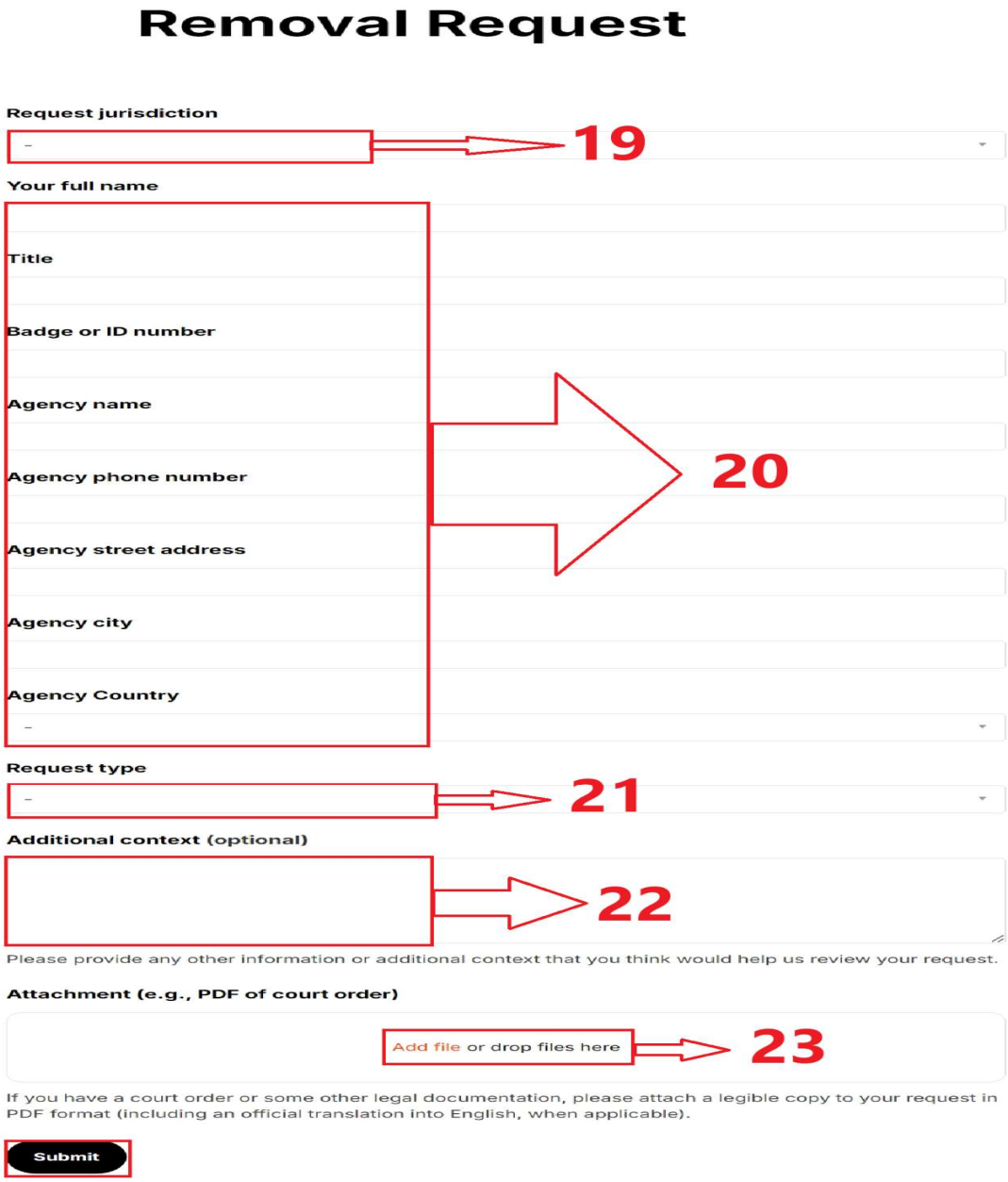
Field 18: **Attachment**: The IO shall attach the signed letter(s) / order(s) in pdf/jpg format and press the submit button.

Information requests shall be submitted, and the status can be accessed on the dashboard.

Removal Request

If the IO wants to make a content removal request, then he may submit it by clicking 'Removal Request', as shown in Field 3 in Picture 5.4. They will be redirected to the Reddit Removal Request Submission Web page as shown in Picture 5.8 below.

Picture 5.8 Removal Request submission dashboard web page



IO needs to submit the following details to submit a Removal request:

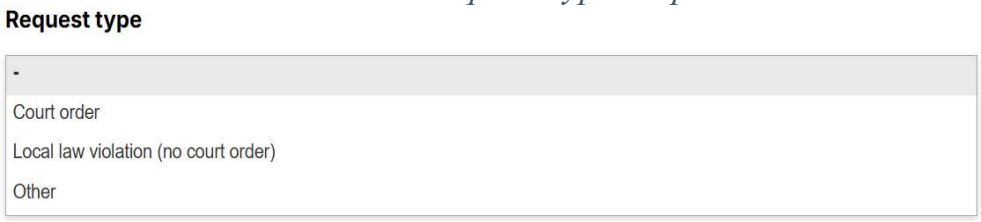
Field 19: **Request Jurisdiction**: the IO fills in jurisdiction where they want the content to be removed, i.e. India.

Field 20: **Full details of the IO**: the IO fills in the full name, title / Rank of the IO, i.e. Sub Insp., Insp. etc., badge number, i.e. PIS No. and phone

number of the IO, as well as other information related to the agency, i.e. Delhi Police.

Field 21: **Request Type**: The IO select crime type from the dropdown 'type of Investigation/Crime' as shown in Picture 5.9

Picture 5.9 Request Type dropdown



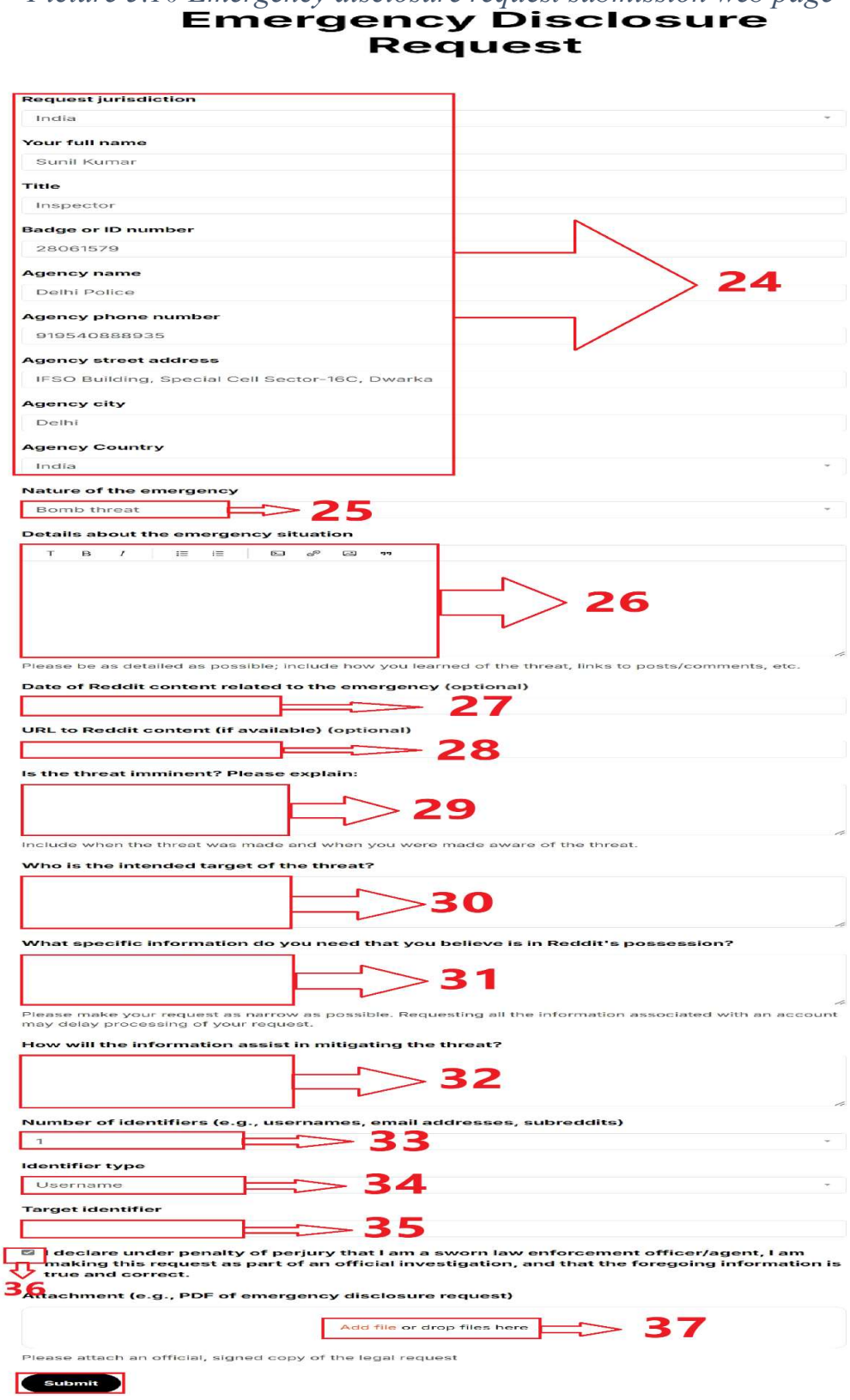
Field 22: **Additional Context**: IO fills in the additional information about the user.

Field 23: **Attachment**: the IO attaches the signed letter(s)/court order(s) in pdf/jpg format and presses the submit button. The content removal request is submitted

Emergency disclosure request:

If the IO wants to make an emergency disclosure request, then he may submit the same by clicking on 'Emergency Disclosure Request' in **Field 4**, as shown in Picture 5.4, and they will be redirected to Reddit Emergency Disclosure Request Submission Web Page as shown in Picture 5.10

Picture 5.10 Emergency disclosure request submission web page



.

Field 24: **Full details of IO**: Full name, the title of the IO, i.e. Sub Insp., Insp. etc., badge number, i.e. PIS No. and the phone number of the IO, as well as information related to the agency, i.e. Delhi Police.

Field 25: **Nature of Emergency**: The IO select the nature of the emergency from the dropdown, as shown in Picture 5.11

Picture 5.11 Nature of emergency dropdown web page



Field 26: **Details about Emergency**: The Investigation Officer fills in the details about the emergency.

Field 27: **Date of content related to Emergency**: In this field, the Investigation Officer fills out the date when they came to know about the emergency. It is optional.

Field 28: **URL of the content**: The Investigation Officer fills up the URL of the reported content.

Field 29: **Is the Threat Imminent**: In this field, Investigation Officer fills up whether the threat is imminent. It has to be explained in detail.

Field 30: **Target of Threat**: In this field, the Investigation Officer fills in about the target of the threat.

Field 31: **Specific Information**: In this field, the IO fills in about the specific information that they want to get from Reddit.

Field 32: **How will Information assist**: IO explains how the information provided by Reddit will help them in mitigating the threat.

Field 33: **Number of Identifiers:** IO selects the number of identifiers (identifier implies users), i.e. 1, 2, 3, etc., in their case, about whom they want information from Reddit.

Field 34: **Identifier Type**: IO selects an identifier, i.e. username, email, or other. (The user name may be available in one case, and in another case, email might be available)

Field 35: **Target Identifier**: IO fills in the details of the identifier, i.e. username, email ID, etc.

Field 36: **Acknowledgment**: In this checkbox, the IO marks tick on the acknowledgement: 'I declare under penalty of perjury that I am a sworn law enforcement officer/agent, I am making this request as part of an official investigation, and that the foregoing information is true and correct'.

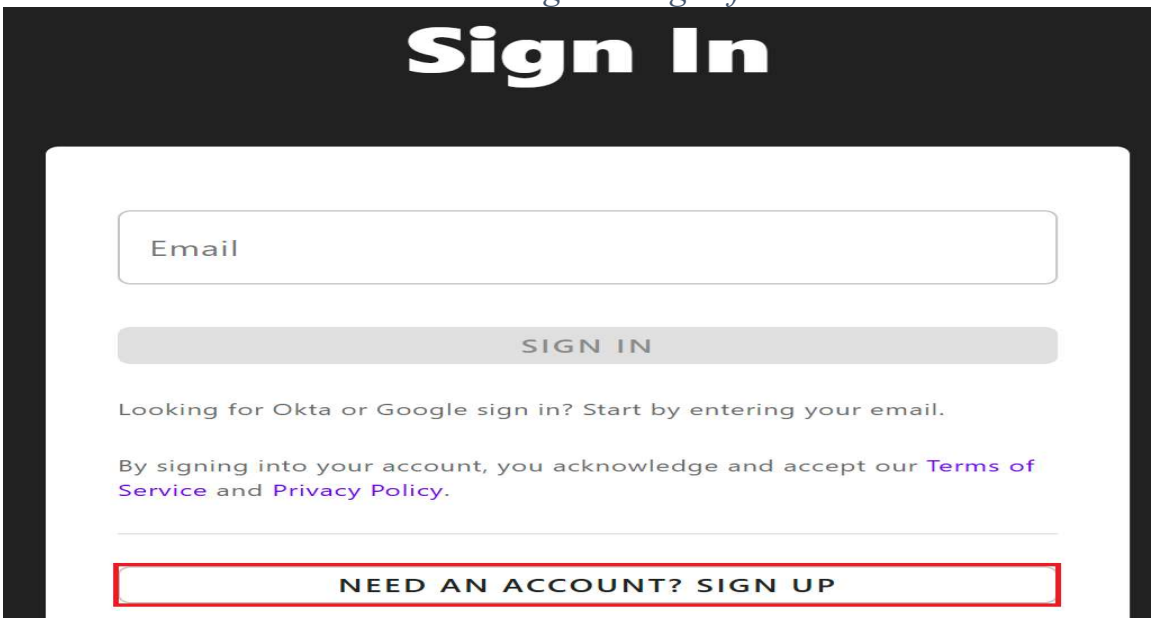
Field 37: **Attachment**: IO attaches the signed letter(s)/court order(s) in pdf/jpg format and presses the submit button. The Emergency disclosure request is submitted.

Chapter 6- LinkedIn Corporation

There is no dedicated portal of LinkedIn corporation for law enforcement agencies. Kodex provides a "Legal Requests" portal for police officers to submit data disclosure requests. This chapter lays down the process for data disclosure requests regarding LinkedIn. The Kodex portal is also adopted by cryptocurrency exchanges, i.e. Binance, Coinbase, Kucoin, etc. To make any data disclosure request, one has to register on the Kodex Portal. The detailed procedure for the Kodex portal:

1. https://app.kodexglobal.com/signin is the URL that an IO can use to submit requests through Kodex. The web page is shown in Picture 6.1.

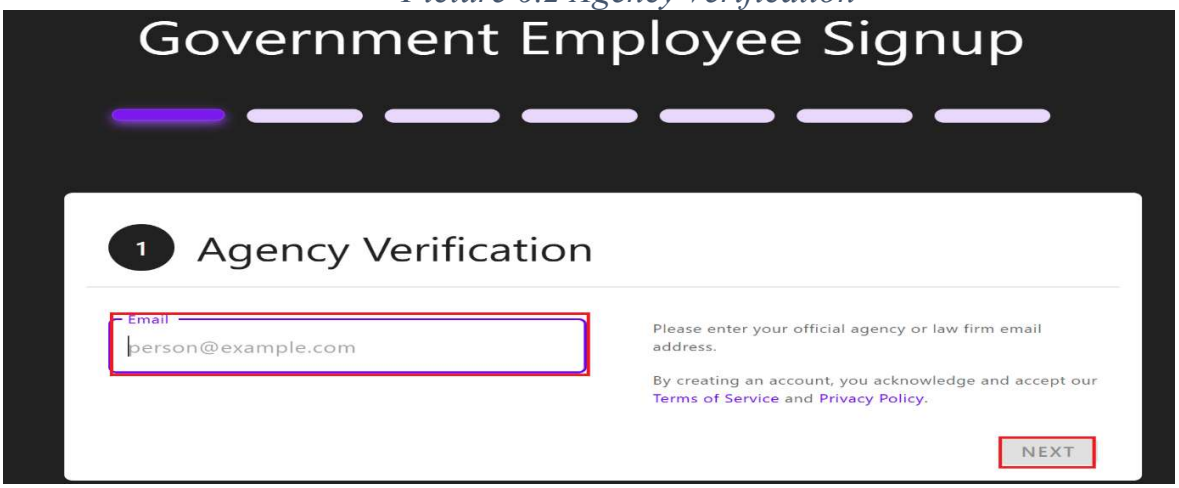
Picture 6.1 Sign-in Page of Kodex



This web page provides secure access to Kodex Portal to sign up. On this page, the concerned IO must sign up to make his official account on Kodex.

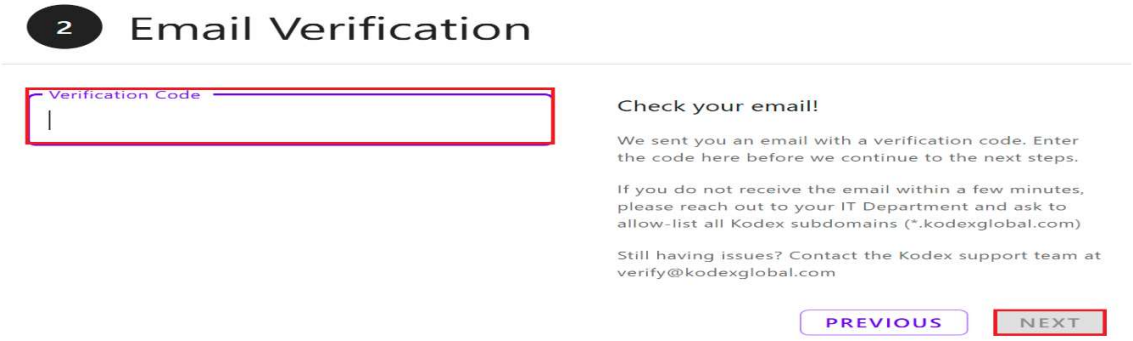
2. The concerned IO visits the portal by clicking on the 'Sign up' button provided on the picture 6.1 Web Page. The following web page (Picture 6.2) opens.

Picture 6.2 Agency Verification



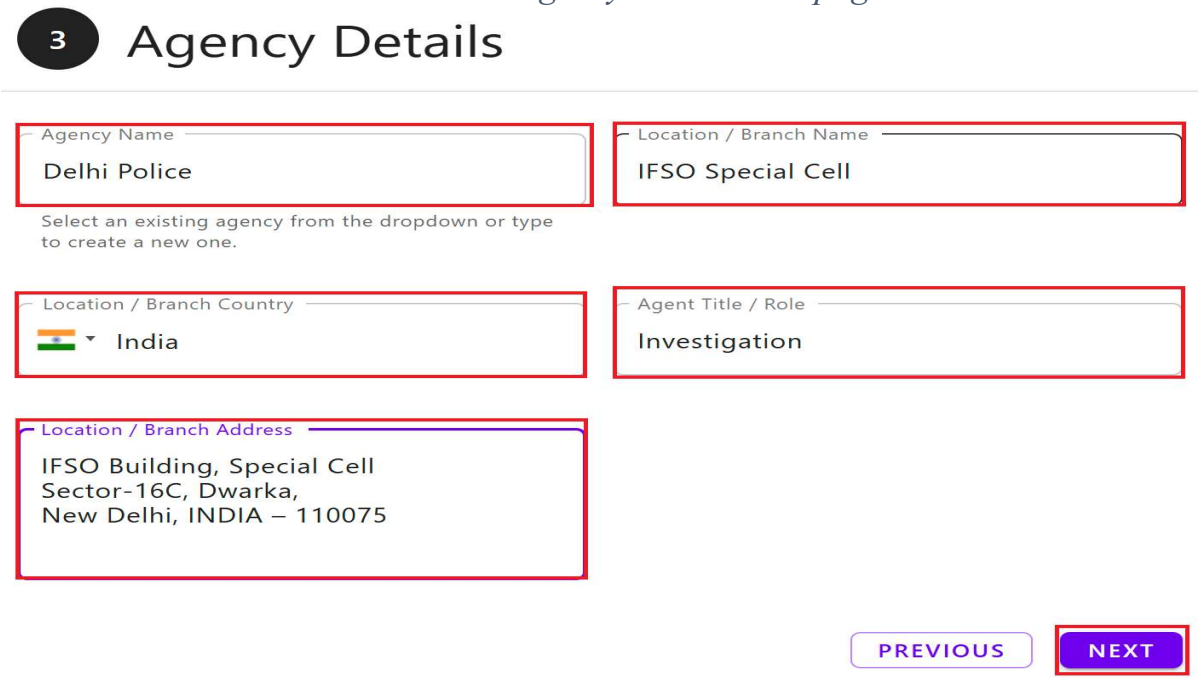
3. The IO fills up the official email ID. After submitting the email ID and clicking on the 'next' button, the concerned IO will get a link from Kodex by email ID no-reply@kodexglobal.com, for which they will get a verification code.

Picture 6.3 Email verification web page.



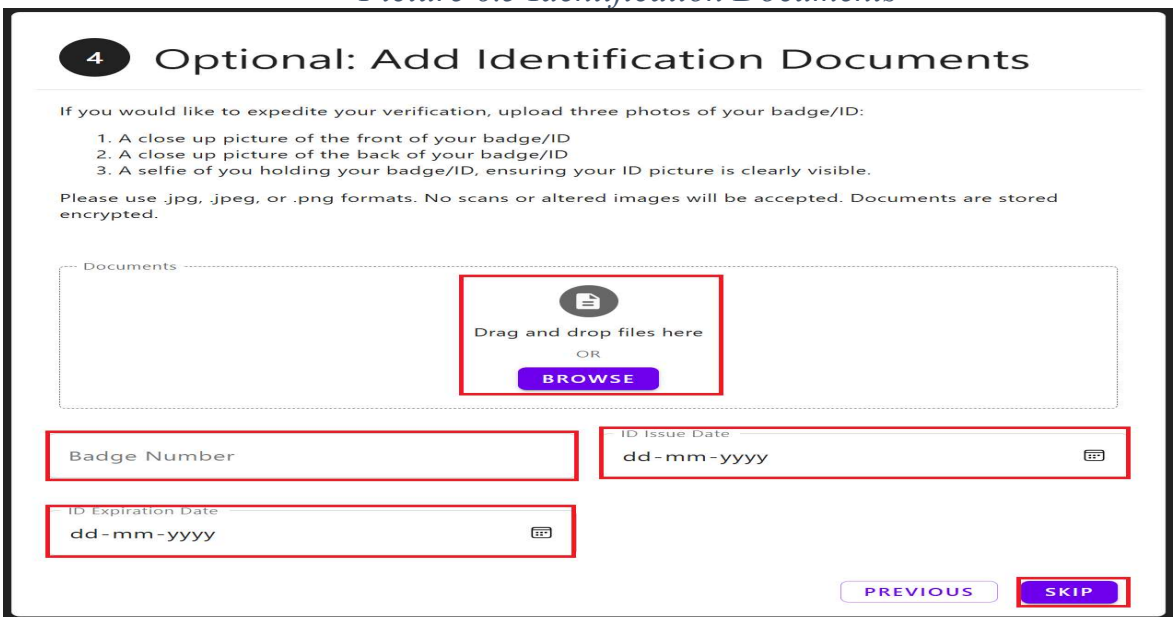
4. The IO fills in the verification code received on their official email ID. After filling in the verification code, the IO presses the 'next' button in Picture 6.3.

Picture 6.4 Agency Details web page



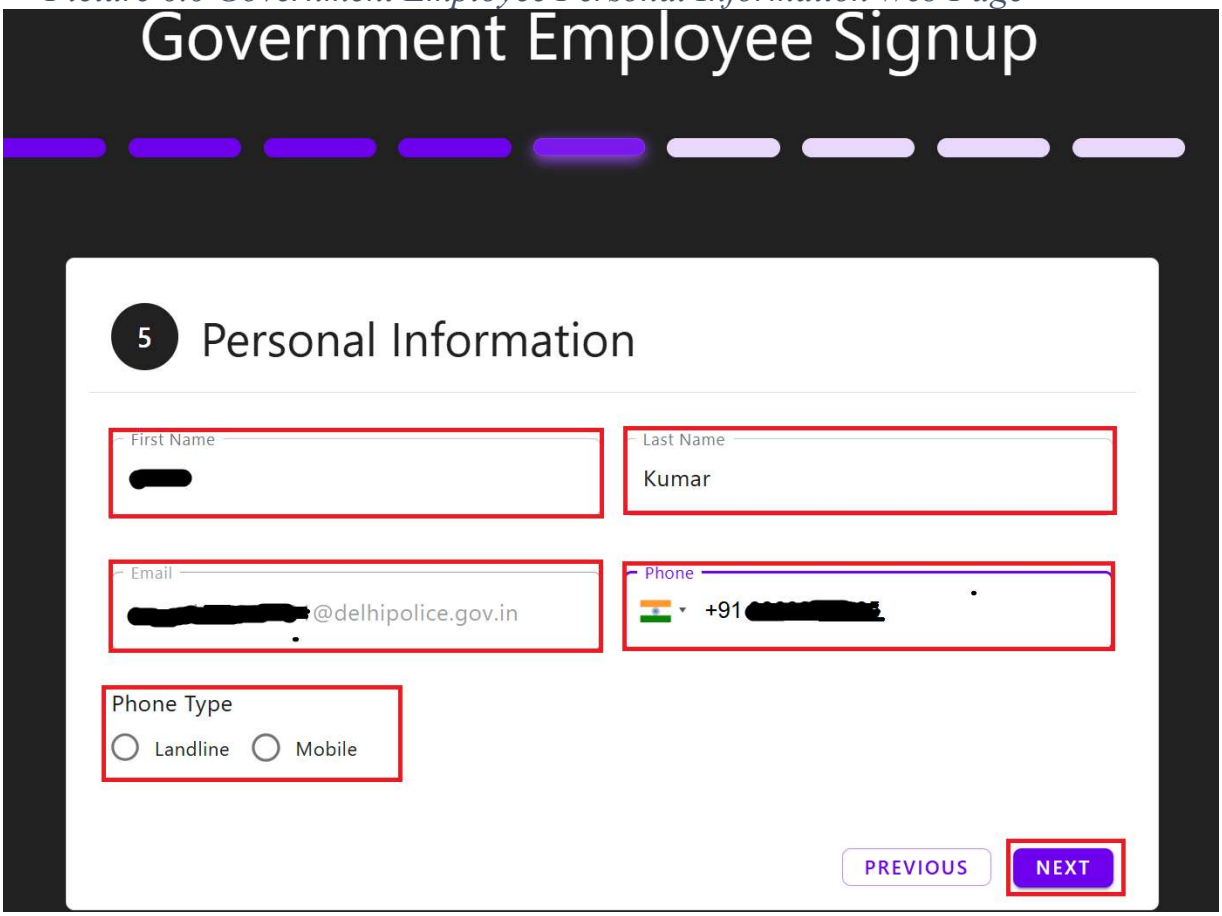
5. The IO fills out the details of their agency, i.e., Delhi Police, location/branch, role, and address. Thereafter, they click the following button at Picture 6.4, and the Picture 6.5 identification web page, as shown below, opens.

Picture 6.5 Identification Documents



6. The Investigation Officer attaches three photos of the front and back of his identity card. He also attaches their selfie with an identity card, as shown in Picture 6.5. He also fills in his PIS No., its issue date, and its expiration date. The date of retirement may be filled out for the expiration date of the identity card. This part is optional, and it may be skipped. However, when it is filled out by the IO, verification is easy for Kodex, and it takes less time than usual.

Picture 6.6 Government Employee Personal Information Web Page



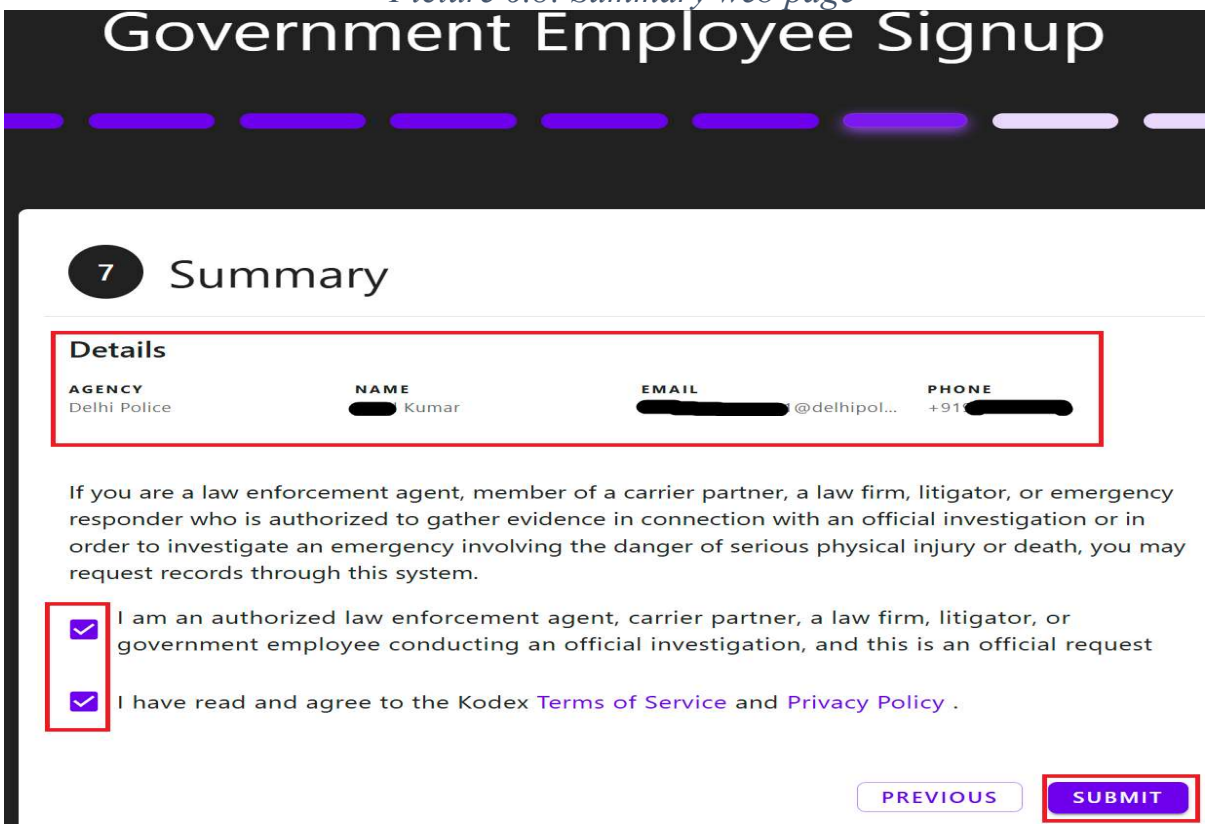
7. The Investigation Officer fills in his personal information, i.e. name, email and phone number, as shown in Picture 6.6 and clicks next. They will find the below-mentioned web page shown in Picture 6.7

Figure 6.7 Referring to the Organization web page



8. The Investigation Officer selects the name of the organisation that referred them to the Kodex Platform, as shown in Picture 6.7. This option may be skipped by clicking skip. The following web page (Picture 6.8) will open: -

Picture 6.8: Summary web page



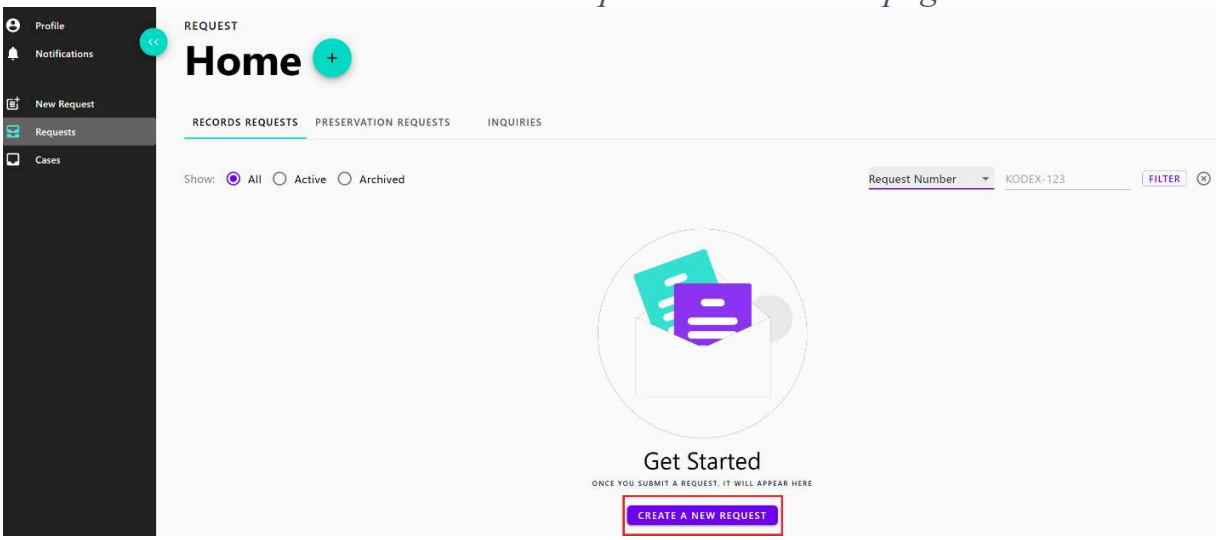
9. The Investigation Officer will find the details in Picture 6.8 filled by them in the 'Details' section. They shall mark a tick in the checkbox, which is an acknowledgement taken from the IO, and press the submit button. The request has been submitted to the Kodex Platform.
10. The Kodex team verifies the submitted request. It takes about 2-3 days to verify the request of IO.
11. After verification, the IO receives the Sign-in link to reset the password for the first time. After resetting the password, the steps are to be followed:
12. Now the IO again opens the link https://app.kodexglobal.com/signin, and below the mentioned web page, as shown in Picture 6.9, will open: -

Picture 6.9 Sign-in Web Page for Investigating Officer



13. After submitting the Email ID and password, the concerned IO (IO) will get a Link from Kodex by email ID no-reply@kodexglobal.com, which will provide him access to the Legal Requests Platform of Kodex and the following web page, as shown in Picture 6.10, will open.

Picture 6.10 New request creation homepage



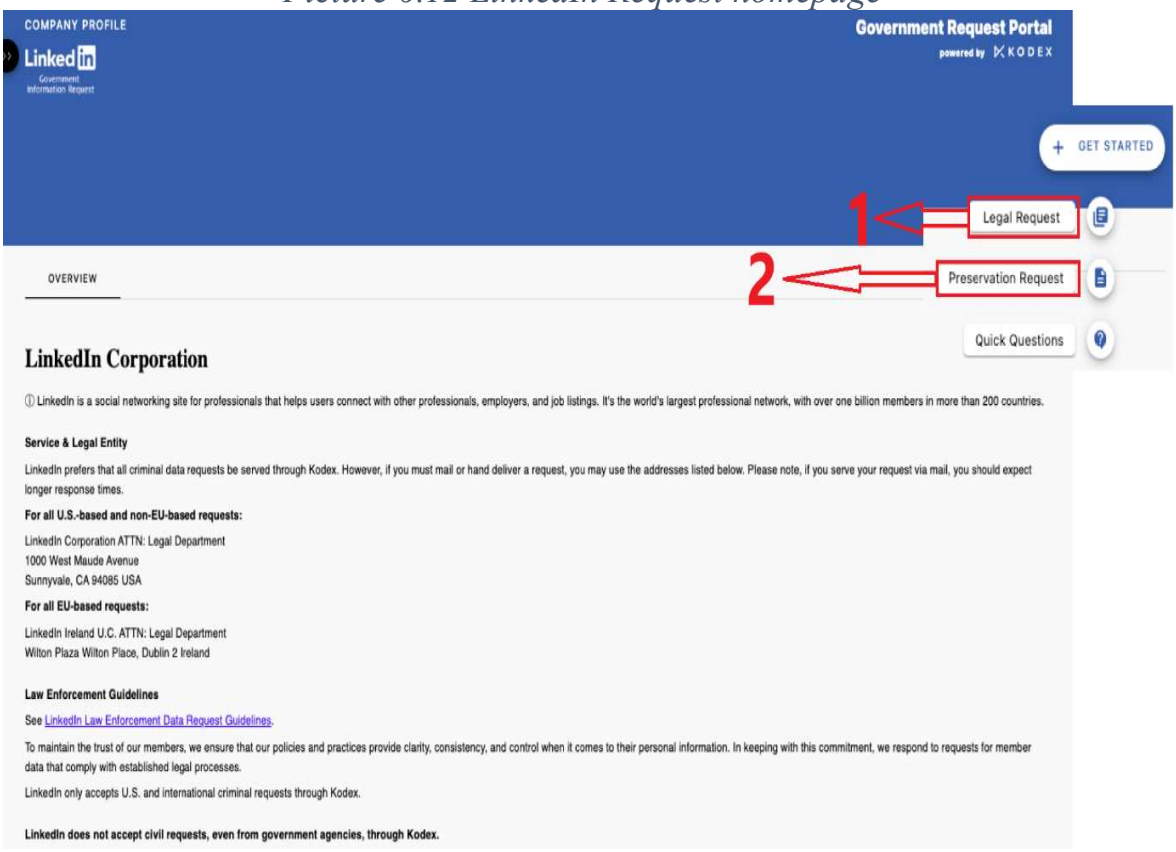
14. The IO Now open the LinkedIn page by clicking on LinkedIn at 'Create a New Request' (as shown in Picture 6.10), and the below page (Picture 6.11) will open:

Picture 6.11 LinkedIn home web page



15. The IO clicks on the LinkedIn box as shown in Picture 6.11 above, and the following web page opens (Picture 6.12):

Picture 6.12 LinkedIn Request homepage

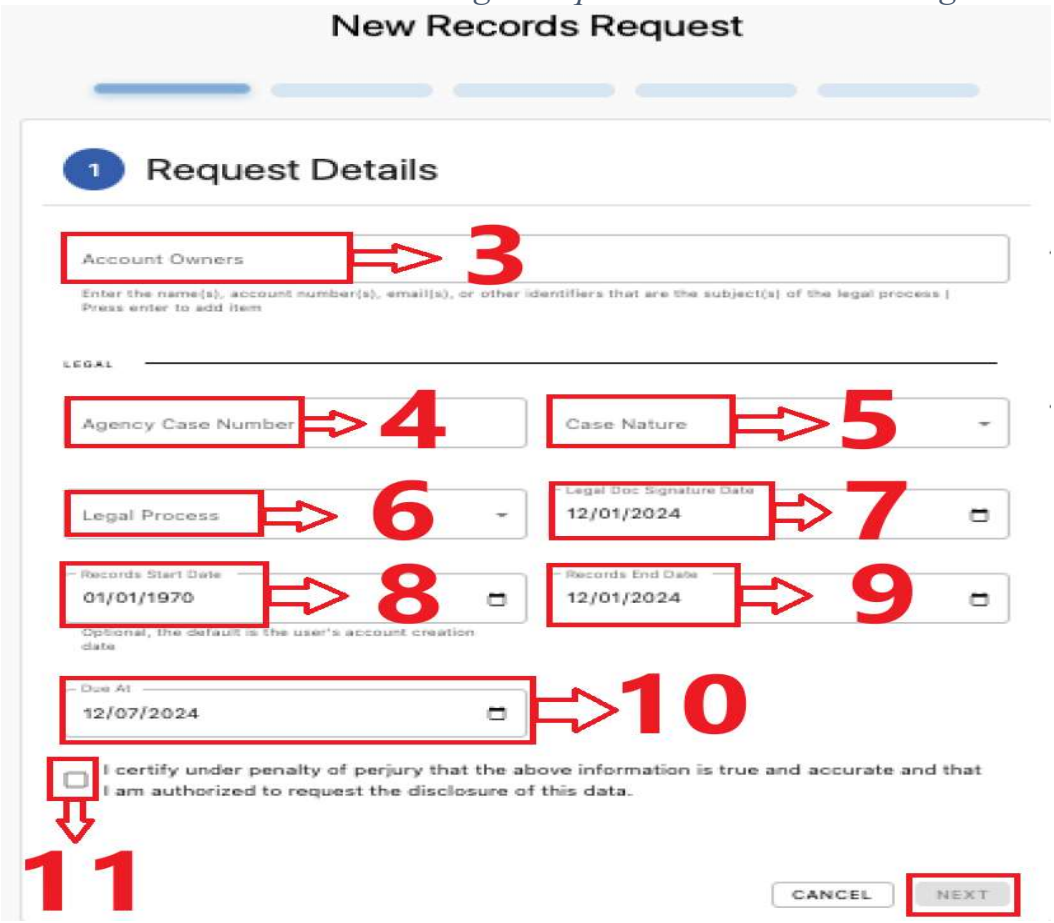


The IO has two options to make separate requests at the above dashboard, as shown in Picture 6.12.

Legal request:

If the IO wants to make a legal request, then he may click on ‘Legal Request’ in Field 1, as shown in Picture 6.12, and they will be redirected to the LinkedIn Legal Request Submission Web page, as shown in Picture 6.13. IO needs to submit the following details to submit a legal request:

Picture 6.13 LinkedIn Legal Request Submission Web Page

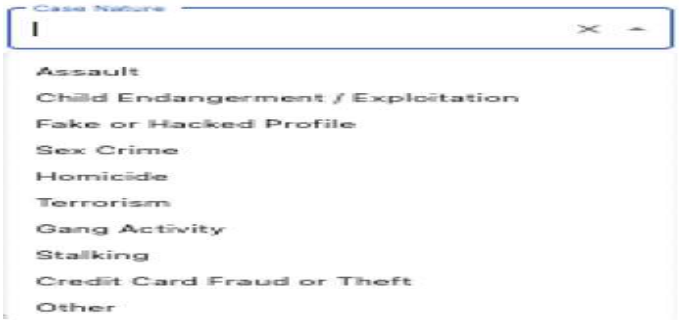


Field 3: **Account owners:** Full name of the account owner.

Field 4: **Agency case number:** In this field, the IO fills out the case/complaint no.

Field 5: **Case nature**: The IO selects the nature of the case from the dropdown mentioned in Picture 6.14.

Picture 6.14 Case Nature dropdown



Field 6: **Legal Process:** The IO selects the legal process from the dropdown mentioned in Picture 6.15.

Picture 6.15 Legal Process dropdown web page



Field 7: **Legal document signature date**: The IO selects the date of the signature on the legal document/notice. It is the date on which the competent authority signed the letter.

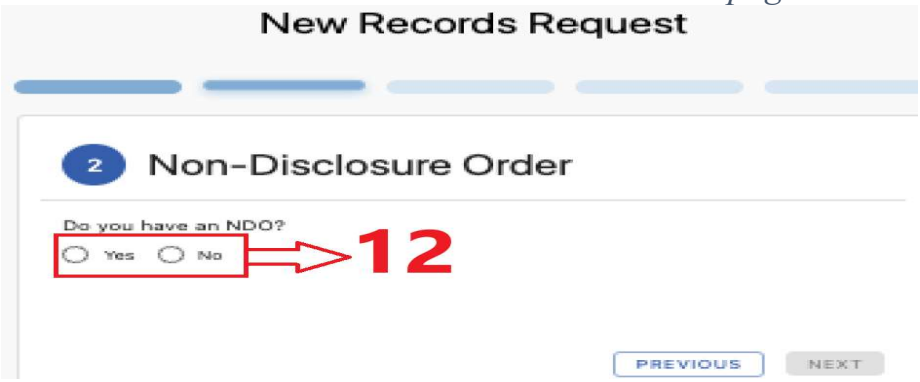
Field 8: **Records start date**: The IO selects the Record start date. It is the date from when they want data from LinkedIn.

Field 9: **Records end date:** The IO fills in the Record end date. It is the date when they want data from LinkedIn.

Field 10: **Record due date:** In this field, IO selects the due date. It is the date on which they want data from LinkedIn.

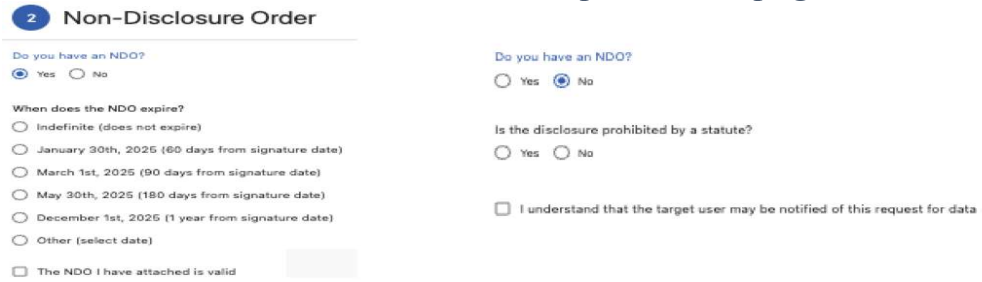
Field 11: **Checkbox for acknowledgement:** In this checkbox, the IO marks tick on the acknowledgement '*I certify under penalty of perjury that the above information is true and accurate and that I am authorised to request the disclosure of this data*' and click next.

Picture 6.16 Non-disclosure order web page

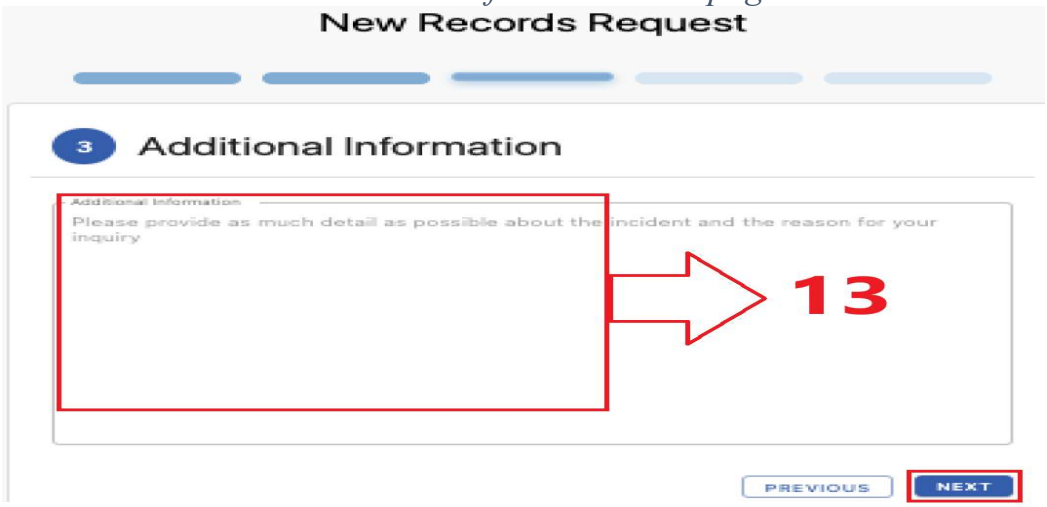


Field 12: **Non-disclosure order**: If the IO has non-disclosure from the competent authority, they click 'yes'; otherwise, click 'no' (Picture 6.16). The following options are available in the yes/no dropdown: If it is not available with the IO, they may leave it blank (Picture 6.17).

Picture 6.17 Non-disclosure order dropdown web page



Picture 6.18 Additional Information web page



Field 13: **Additional Information:** In this field, the IO fills up as many details as possible about the incident and the reason for their request, as shown in Picture 6.18.

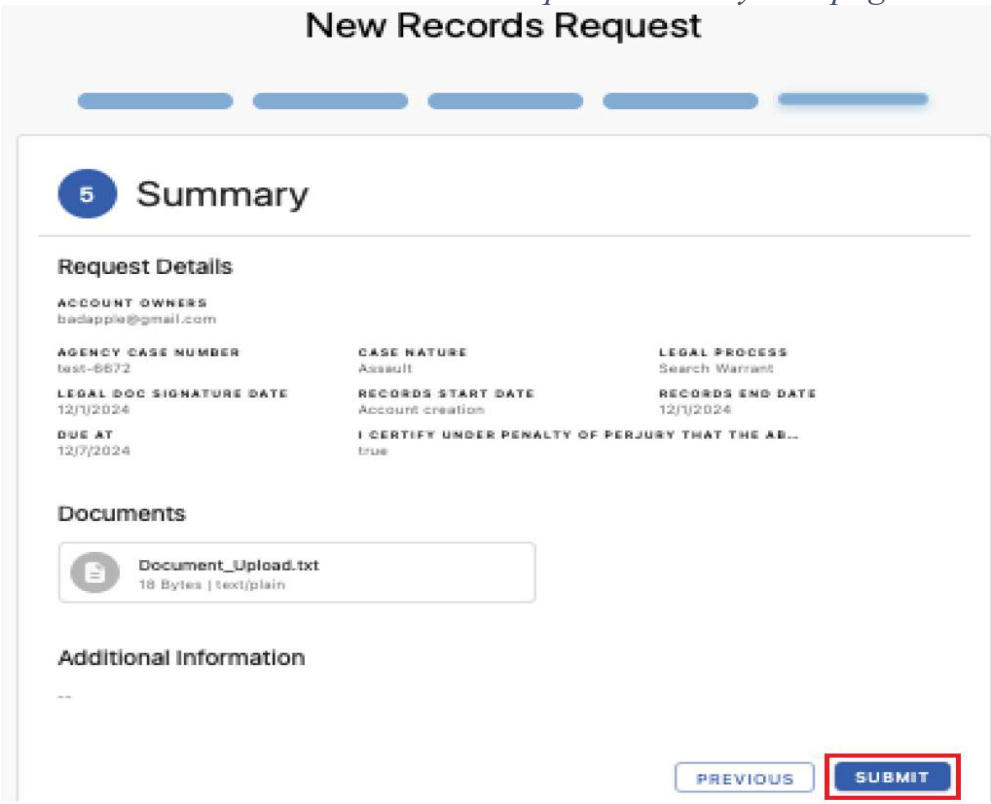
Picture 6.19 File attachment web page



Field 14: **Attachment:** In this field, the IO attaches the signed letter(s)/order(s) in pdf/jpg format. They may send five files at a time. If they want to send more than five files, then they should put these files in a zip folder and attach them here. Then click on the next button, as shown in Picture 6.19.

Thereafter, the web page, as shown in Picture 6.20, opens. The IO can check the summary thoroughly, and if any correction is needed, he may make it. Otherwise, he may click the submit button, and the request is submitted.

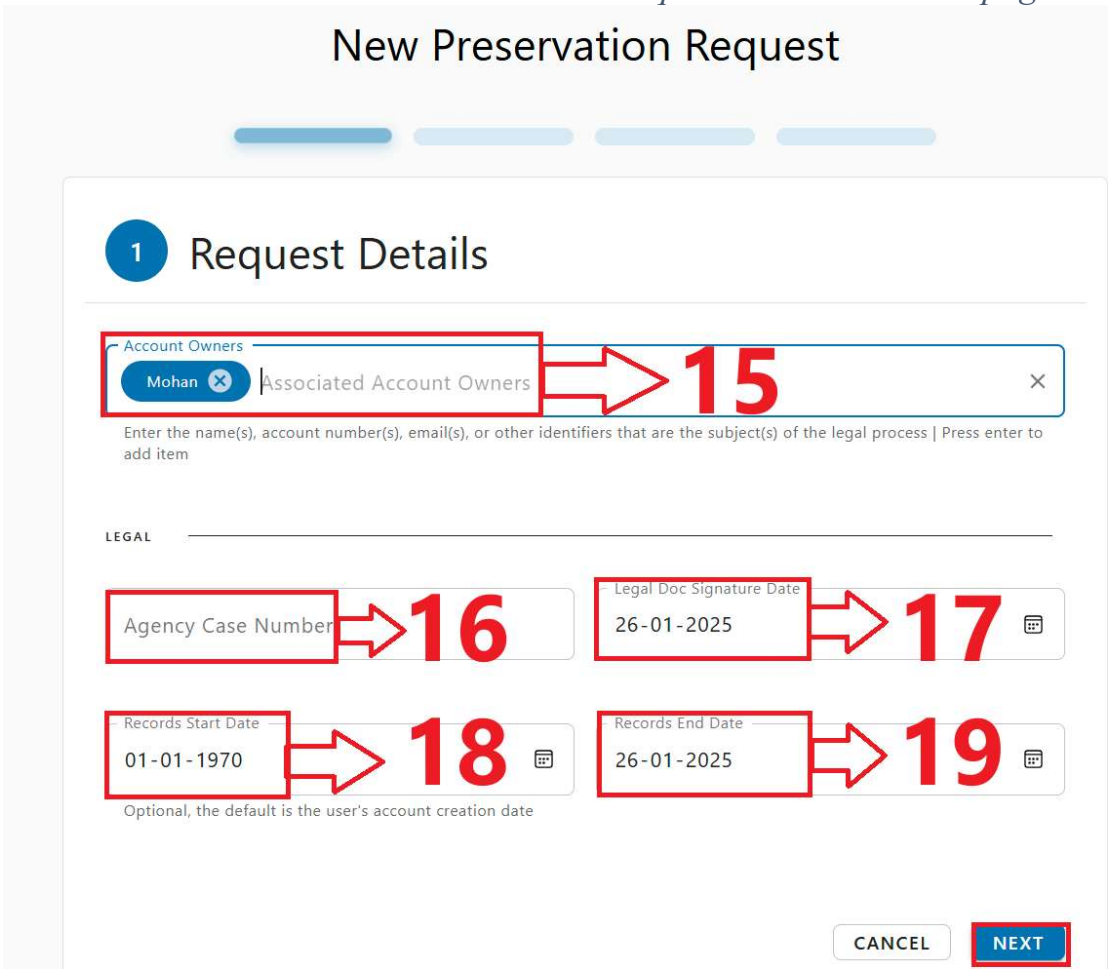
Picture 6.20 New Record Request summary web page



Preservation request:

If the IO wants to make a Preservation request, then he may click on ‘Preservation Request’ in Field 2, as shown in Picture 6.12, and they will be redirected to the LinkedIn Preservation Request Submission Web page, as shown in Picture 6.21.

Picture 6.21 LinkedIn Preservation Request Submission Web page



The IO needs to submit the following details to submit a preservation request.

Field 15: **Account owners**: Enter the name/account number/email ID or any other identifier of the subject's account.

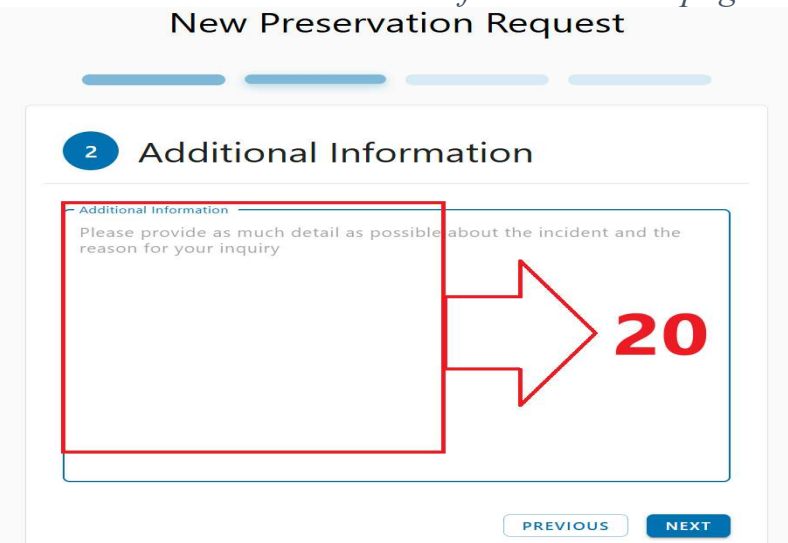
Field 16: **Agency Case number**: The IO shall enter the case /complaint no. of their case.

Field 17: **Legal document signature date:** The IO shall select the date on which the competent authority signed the letter.

Field 18: **Records start date:** The IO shall enter the date from when they want data from LinkedIn.

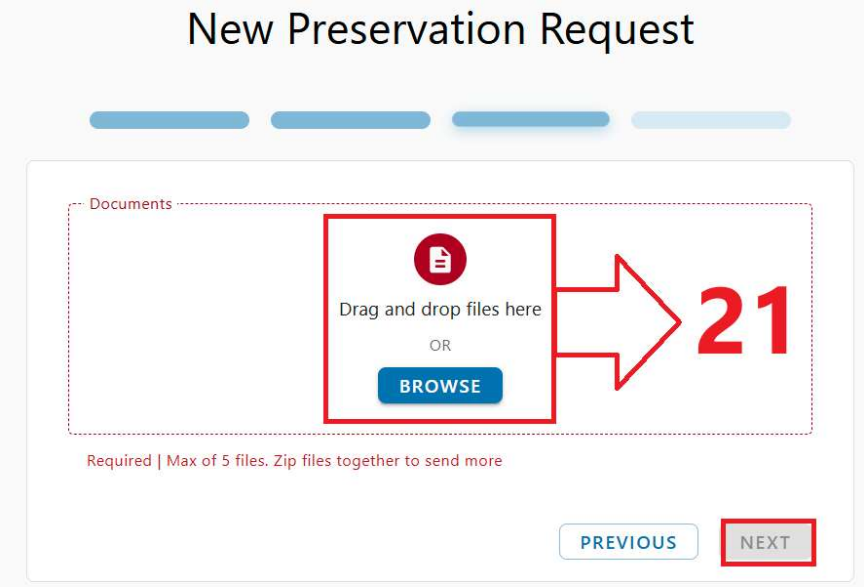
Field 19: **Records end date**: The IO shall select the date when they want data from LinkedIn. Thereafter, the IO clicks on the 'next' button shown in Picture 6.21.

Picture 6.22: Additional Information web page



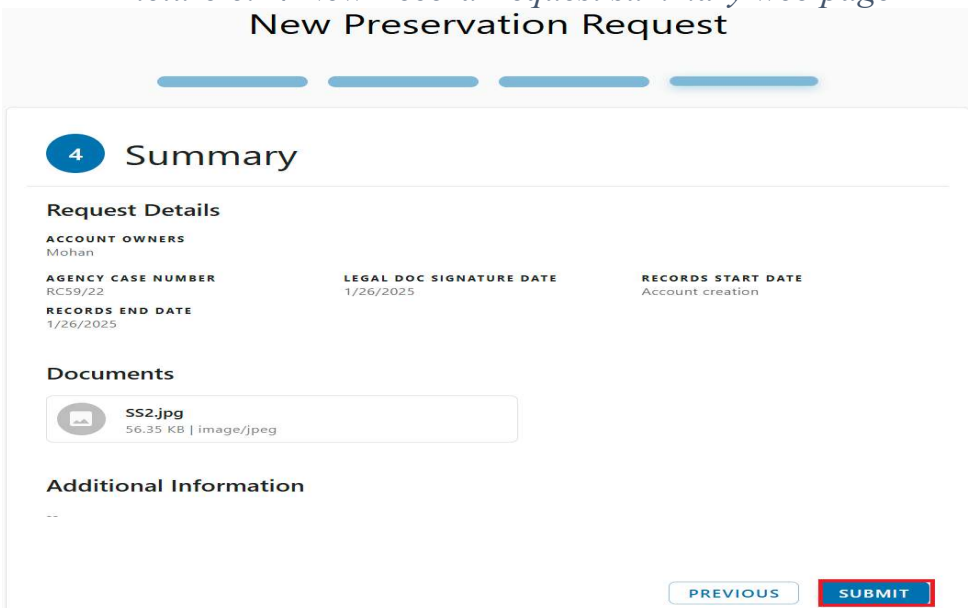
Field 20: **Additional Information:** IO fills up as many details as possible about the incident and the reason for their request, as shown in Picture 6.22

Picture 6.23: File attachment web page



Field 21: **Attachment**: The IO attaches the signed letter(s)/order(s) in pdf/jpg format. They may attach five files at a time. If they want to send more than five files, then they should put these files in a zip folder and attach them here. Then click on the next button, as shown in Picture 6.23.

Picture 6.24 New Record Request summary web page



Thereafter, the web page, as shown in Picture 6.24, opens. The IO can check it thoroughly, and if any correction is needed, he may make it. Otherwise, he may click the submit button, and the request is submitted.

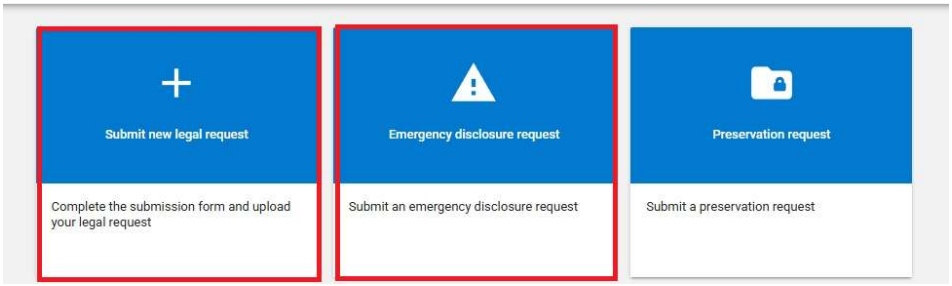
The IO may check the status of their request by logging in to the Kodex Portal and following the procedure mentioned above.

Chapter 7- Google LLC.

The process for data disclosure requests for Google, LLC is via a 'Law Enforcement Online Requests' portal. This portal can be accessed only by the designated authorities of the Delhi Police Districts / Units and Cyber Police Stations. The IOs have to send their requests to the office of their designated authorities. The designated authorities can submit new legal requests and emergency disclosure requests on this portal. The following steps are to be followed:

1. https://lers.google.com/ is the URL of the Google LLC Data Disclosure Requests Portal. The web page is shown in Picture 7.1. This platform is commonly referred to as LEOR (Law Enforcement Online Requests).

Picture 7.1: Law Enforcement Online Request Web Page



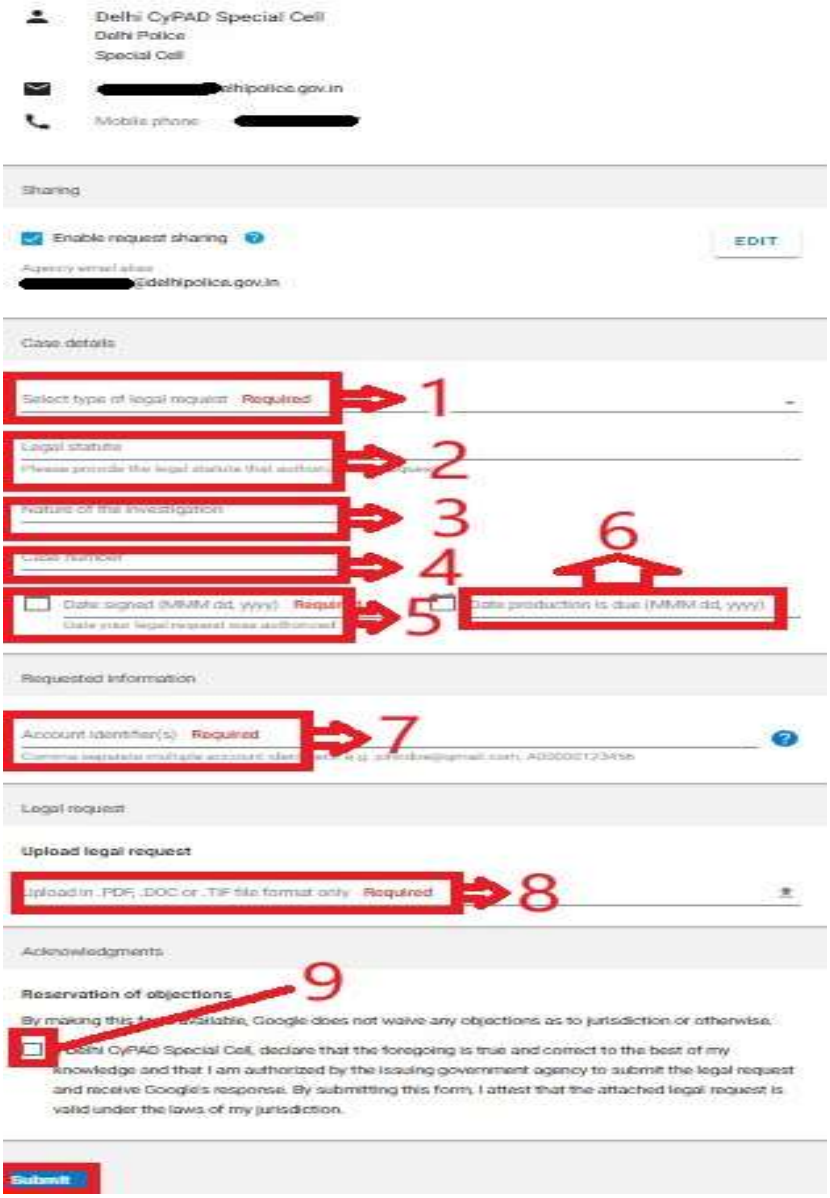
   This web page provides secure access to the Google Law Enforcement Online Request system to submit New Legal Request and Emergency Disclosure Request and Preservation Request.

2. On this Web Page (Dashboard), a New Legal Request or Emergency disclosure Request can be made. Google locks the preservation request option. Hence, this request cannot be made.

To Make a Legal Request

When the Designated Officer (IO) clicks on “Submit New Legal Request” on the request dashboard on the Requests Web Page (shown in Picture 7.1 above), a new Web Page will open as shown in Picture 7.2 below

Picture 7.2: Legal Request Submission web page



The IO needs to submit the following details to submit a new Legal request

Field 1: **Type of Legal Request** refers to Police Request, Prosecutor request, Court order, Emergency disclosure request or Other Government Request. It has to be chosen from the dropdown, as shown in Picture 7.3.

Picture 7.3: Type of Legal Request



Field 2: **Legal Statute** refers to the section of law by which a legal request is being made from Google LLC.

Field 3: **Nature of the Investigation**: The Designated Officer selects the nature of the investigation from the dropdown, as shown in Picture 7.4

Picture 7.4 Type of Investigation



Field 4: **Case Number** refers to the internal case/complaint number that is being investigated/enquired.

Field 5: **Date Signed** refers to the date on which the competent authority signed the notice/court order.

Field 6: **Due Date of Production** refers to the date on which the data is required from Google.

Field 7: **Account Identifier** refers to the email ID, username, etc., of the account holder about which information is being sought.

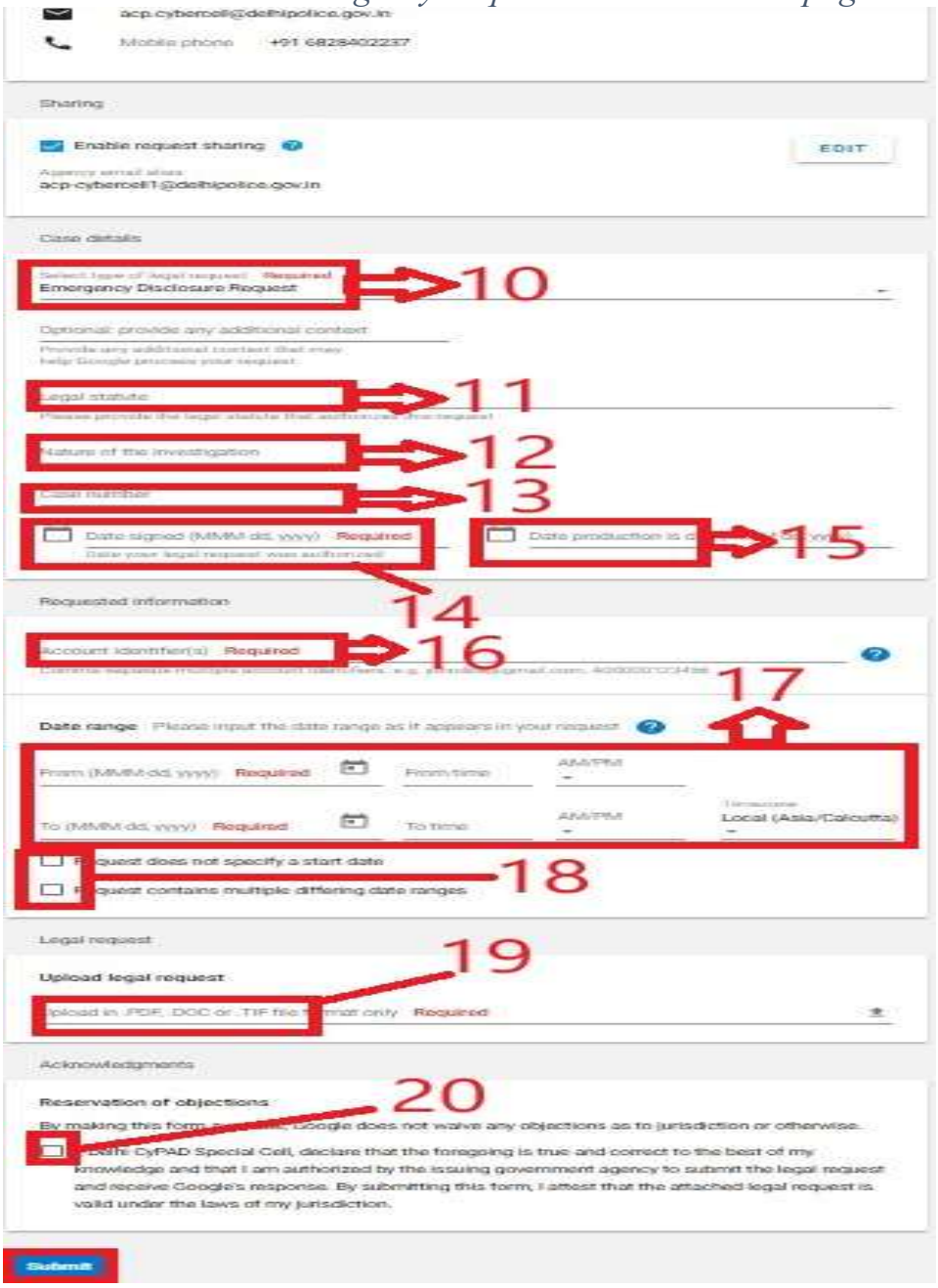
Field 8: **Upload Legal Request** In this section, the Designated Officer attaches the legal signed letter/order in pdf/tif format.

Field 9: **Checkbox** By clicking this checkbox, the Designated Officer acknowledges that he is an authorised Officer and that all the information he has submitted is accurate. Thereafter, as the submitted button is clicked, the Legal Request is submitted to Google.

To Make an Emergency Disclosure Request

When the Designated Officer clicks on the Emergency Disclosure Request button on the Requests Dashboard (shown in Picture 7.1 above), a new Web Page will open, as shown in Picture 7.5 below.

Picture 7.5: Emergency Request Submission web page

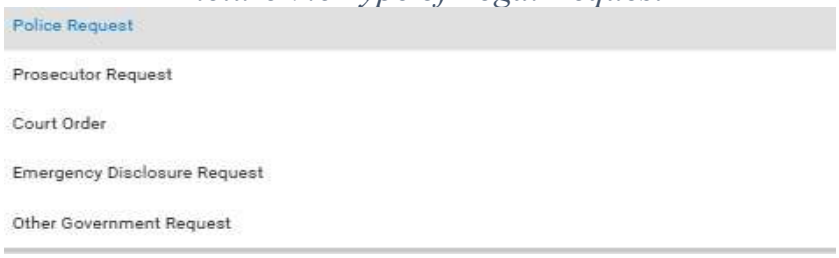


The Designated Officer needs to submit the following details to submit an Emergency Disclosure request:

Field 10: **Type of Legal Request** refers to Police Request, Prosecutor request, Court order, Emergency disclosure request or other Government

Request. It has to be chosen from the dropdown, as shown in Picture 7.6.

Picture 7.6 Type of Legal Request



Field 11: **Legal Statute** refers to the section of law by which a legal request is being made from Google LLC.

Field 12: **Nature of the Investigation**: In this field, the Designated Officer selects the nature of investigation from the dropdown, as shown in Picture 7.7

Picture 7.7 Type of Investigation



Field 13: **Case Number** refers to the internal case/complaint number that is being investigated/enquired.

Field 14: **Date Signed** refers to the date on which the competent authority signed the legal notice/court order.

Field 15: **Due Date of Production** refers to the date on which the data is required from Google.

Field 16: **Account Identifier** refers to the email ID, username, etc., of the account holder about which information is being sought in an emergency.

Field 17: **Date Range** refers to the duration for which the information is being sought in an emergency. The Designated Officer has to fill in the start date and time to the end date and time. The time zone has also to be selected, i.e., Asia and Kolkata.

Field 18: **Check box**: The Designated Officer ticks in the appropriate box whether the request contains multiple different dates or not.

Field 19: **Upload Legal Request:** In this section, the Designated Officer attaches the legally signed letter/order in pdf/tif format.

Field 20: **Checkbox:** By clicking this checkbox, the Designated Officer acknowledges that he is an authorised Officer and that all the information he has submitted is accurate. Thereafter, as the submitted button is clicked, the Legal Request is submitted to Google.

Data provided by Google

1. Personal Details: Name, phone number, recovery email, IP address and login account creation details
2. Records of searches performed by the user through Google Search, data associated with Chrome (if synced to a Google account), including browsing history and bookmarks
3. Videos uploaded, watched, liked, or commented on YouTube
4. Files stored in Google Drive, including shared files and activity logs
5. Location history: check-ins and places visited (Data from Google Maps and Google Places)
6. Lists of contacts synced to the Google account

7. Devices linked to the account, including device IDs, make, model, and last used location
8. Apps downloaded or purchased from the Google Play Store
9. Details of transactions, including recipient, amount, and date from Google Pay Records, purchase history by using Google services, etc

Chapter 8- Telegram FZ-LLC

Telegram-FZ, LLC accepts data disclosure requests via mail communication only. There is a dedicated mail ID for India: abuse-in@telegram.org. The procedure involves emailing a letter/Notice to the Delhi Police on the letterhead. Mention the following points in the letter/notice:

1. Gist of the case with FIR/Complaint no., date and sections.
2. User account name(s).
3. The letter/Notice should be signed and stamped along with the following supporting documents:-
    i) Screenshots of chats/messages of unlawful activity or/and
    ii) Copy FIR with account names if registered in the case or/and
    iii) Any proof that the user is involved in the mentioned unlawful activity.
4. Mention the data you want from Telegram very clearly in your queries. Some examples of data requests are:
    i) Phone Number, username, profile picture, bio, and any publicly visible information
    ii) Account creation date and time
    iii) List of contacts saved by the user
    iv) Groups to which the user is a member or admin
    v) Channels the user has created or follows and its participants
    vi) IP addresses used for logins, device model, operating system
    vii) User's last-seen status
    viii) Sender and recipient details (usernames and phone numbers, File sizes, types, and timestamps shared/received by the user, live or static locations shared by the user)

ix) Bots created by the user and their log details, data on bots created by the user, etc.

The email should be sent from the email ID of the designated ID of SHO/ACP of the concerned unit/branch, which is non-transferable after the official transfer. Personal government email IDs of the officials should be avoided.

Chapter 9- Information Furnished

Social media intermediaries can provide various types of data. While some data sets are specific to certain platforms, the following information is generally available from all social media intermediaries:

1. Subscriber information:
    a. The subscriber's account or login name.
    b. The subscriber's name and street address;
    c. The subscriber's telephone number(s);
    d. The subscriber's email address(es);
    e. The IP address used by the subscriber to register the account or otherwise to initiate service;
    f. IP logs with session times, dates and durations of the subscriber to log into the account;
2. Transactional information:
    a. IP logs with MAC address(es) of the computer systems to which he was connected during the relevant period.
    b. Connection destination or source of connection, including source port.
    c. Method of connection to system (e.g., telnet, FTP, http)
    d. Data transfer volume (e.g., bytes); and
    e. Any other relevant routing information;
3. Contents Information:
    a. Written Messages, embedded photographs or images, attached files, etc.
    b. Information pertaining to any image(s) or other document(s) uploaded to the account or the website, including the dates and times of uploading and the sizes of the files.

c. Name and other identifying details of individuals that accessed a specific image/file/web page within a specified period on a specified date.
d. Payment and Transaction Data: Details of purchases or financial transactions conducted by using the payment services of the Social Media Intermediary.

4. Location Information:
    a. Location data based on IP addresses or location services, if enabled.
    b. Specific locations shared by the user in the application.
    c. Search History: What the user has searched for within the application.

Chapter 10- Dos and Don’ts

The following Dos and Don’ts must be maintained while sending requests

Dos

- **Be Specific**: Clearly define the data you are requesting and the purpose of the request.
- **Provide Legal Basis**: Ensure you have a valid legal basis for the request, such as a court order or notice. However, it is not necessary in **emergency cases**
- **Follow Proper Channels**: Submit the request through the designated legal channels or portals provided by the platform.
- **Be Timely**: Submit requests promptly to avoid delays in the investigation or legal process.
- **Maintain Confidentiality**: Handle all data and information with strict confidentiality to protect privacy.
- **Document Everything**: Keep detailed records of the request, including dates, communications, and responses.
- **Observe Response Timeframes**: Always follow up within the specified timeframes to ensure compliance. Note down the reference no. or ticket no. (if provided) by the social media intermediary and use it in such follow-ups with social media intermediaries

Don'ts

- **Avoid Ambiguity**: Requests should not be vague or open-ended; specify exactly what data is needed.
- **Respect User Privacy**: Never request personal data without clear, justified reasons
- **Limit Data Requests**: Do not ask for excessive or irrelevant data beyond what is necessary for the case
- **Avoid Informal Language**: Keep communication professional and formal
- **Avoid Blanket Requests**: Be as specific as possible to avoid overburdening the recipient with excessive data processing

****