



DATA REQUEST GUIDELINES

This document describes procedures law enforcement authorities and individuals involved in civil litigation should follow to request data from LinkedIn and its affiliated service providers.

Note: The Guidelines are provided for informational purposes only. LinkedIn may revise the Guidelines at any time and reserves the right to respond or object to any Data Request in any manner consistent with applicable law.

UPDATED December 18, 2020

1. LinkedIn's Commitment to its Members.

To maintain the trust of our Members, we strive to ensure that our policies and practices provide clarity, consistency, and control when it comes to their personal information. In keeping with this commitment to our Members, we respond to requests for Member data in accordance with our Terms of Service, and require that such requests comply with established legal processes. Read more about the requests we receive, and how we keep our Members informed, in our [Transparency Report](#).

2. What types of Data Requests can I make?

We consider only the following types of Requests:

- **Data Requests:** A Data Request is a request for information or documents relating to Member accounts in connection with official criminal investigations or other official legal proceedings. Except in limited emergency situations (see below), we require Data Requests to be made through formal legal process and procedures, and we respond to such requests as required by law. Examples of Data Requests include:
 - Subpoenas
 - Court Orders
 - Search Warrants
 - Other forms of formal legal process, such as requests issued pursuant to a Mutual Legal Assistance Treaty (MLAT) (international Requests are addressed below) or Irish legal process and procedures.

- **Preservation Requests:** A Preservation Request asks LinkedIn to preserve Member account records in connection with official criminal investigations or other official legal proceedings. Preservation Requests must:
 - Identify the account(s) at issue (see No. 4, below, for further details)
 - Identify the investigating agency and/or specific pending official proceedings (signed Requests on law enforcement letterhead preferred)
 - Include assurances that the requesting agency or individual is taking steps to obtain appropriate legal process for access to the data that we are being asked to retain
 - Include a valid return email address

LinkedIn Data Request Guidelines

When we receive a valid Preservation Request we will preserve a one-time snapshot of then-existing account records for 90 days, pending service of formal legal process.

- **Emergency Requests:** Emergency Requests for Member information must be made using the Emergency Disclosure Request Form at the end of these Guidelines. Emergency Requests are only appropriate in cases involving serious bodily harm or death, and we respond to such Requests only when we believe in good faith that such harm may imminently occur if we do not respond without delay.

The Emergency Disclosure Request Form must be submitted by a law enforcement officer and signed under penalty of perjury. (Please see below). Others aware of an emergency situation should contact their local law enforcement officials.

3. What contact information must I provide in my Request?

To help us ensure that Data Requests are from legitimate law enforcement authorities, we require each Data Request to include the following information:

- Requesting Agency Name
- Requesting Agent Name
- Requesting Agent Badge/Identification Number
- Requesting Agent Employer-Issued E-mail Address
- Requesting Agent Phone Number (including extension)
- Requesting Agent Mailing Address (P.O. Box will not be accepted)
- Requested Response Date (allow at least 20 business days for processing)

For other Data Requests in connection with official legal proceedings (e.g., civil litigation), we require that the requesting party ensure that the request clearly identify the requesting party and provide the following contact information for the requesting party and/or its counsel of record:

- Name
- Company or Agency, if applicable
- E-mail Address
- Phone Number
- Mailing Address (P.O. Box will not be accepted)
- Requested Response Date (allow at least 20 business days for processing)

LinkedIn Data Request Guidelines

4. What information must be included in a Data Request?

LinkedIn requires each Data Request to identify the account(s) subject to the request by providing the following information. Without this information, we will be unable to fulfill the request:

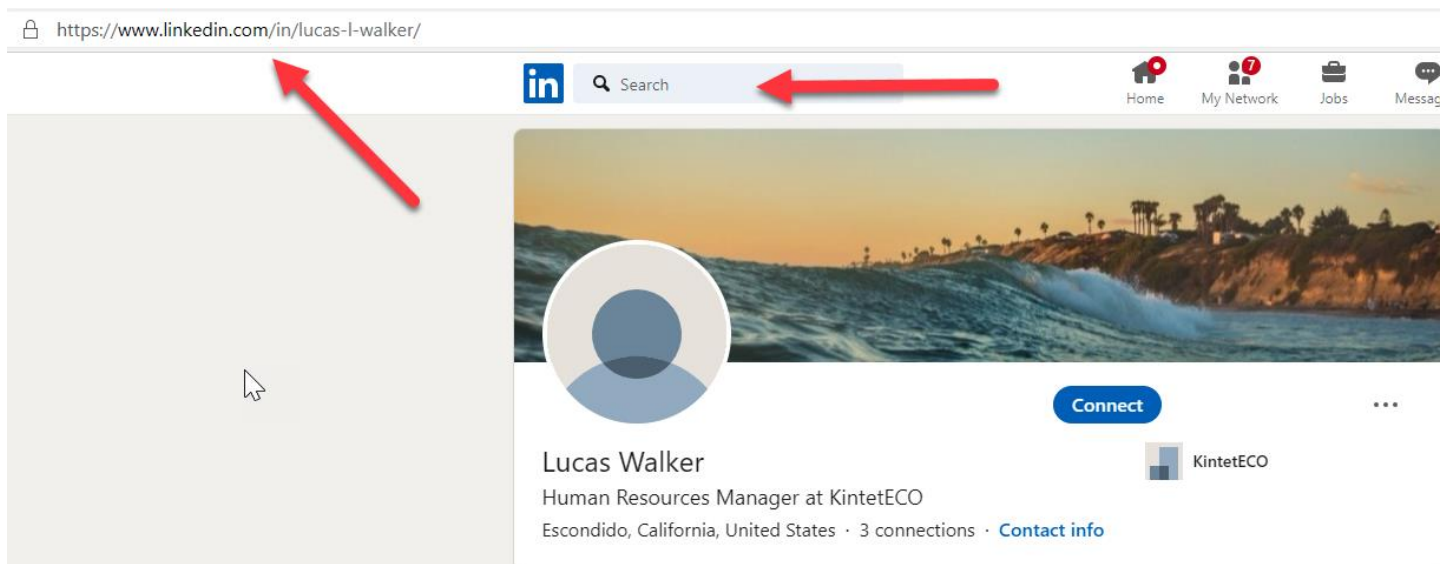
- The full (first and last) name of the LinkedIn Member and email address associated with the account; or,
- The LinkedIn public profile URL.

Please note that LinkedIn public profile URLs come in 2 formats:

- Public Profile URL, for example: <http://www.linkedin.com/in/rufufia-mae-a661234b>; and,
- Customized Public Profile URL, for example: <http://www.linkedin.com/in/patrickwest1283>

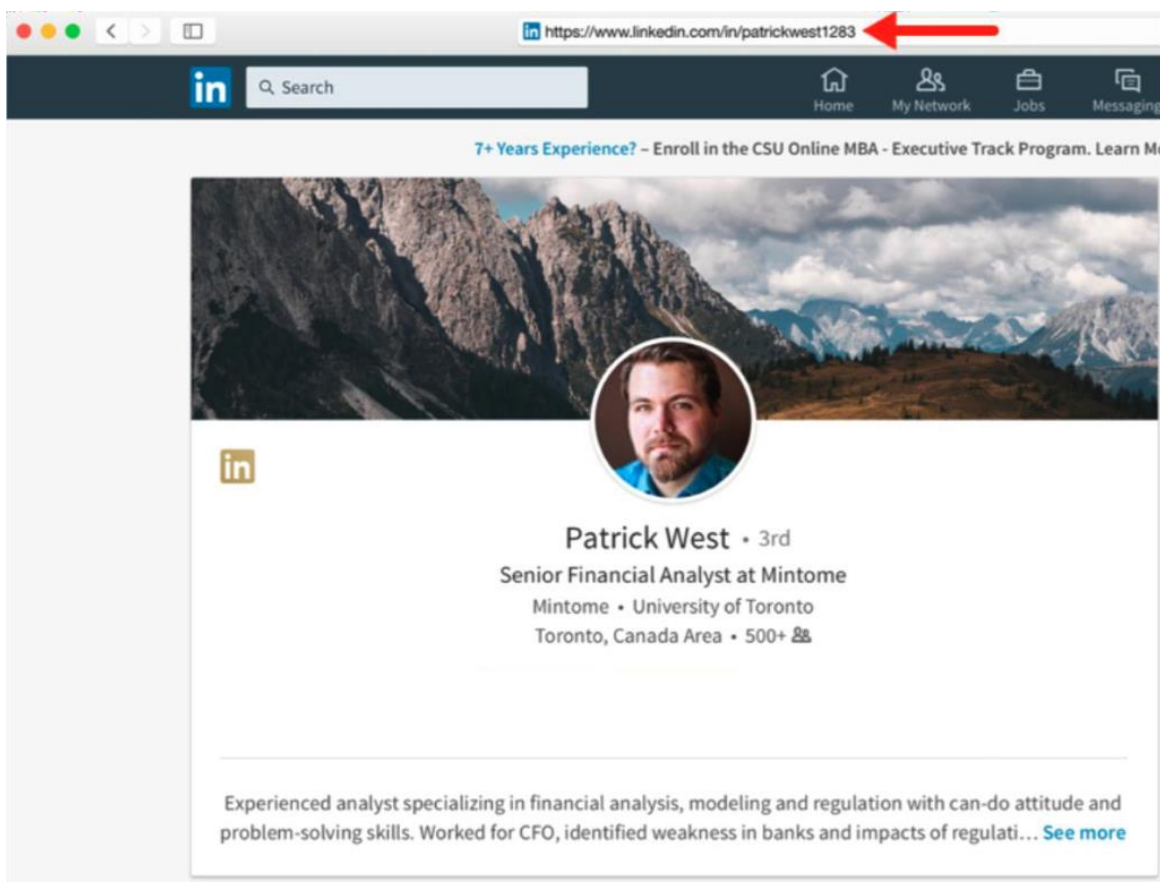
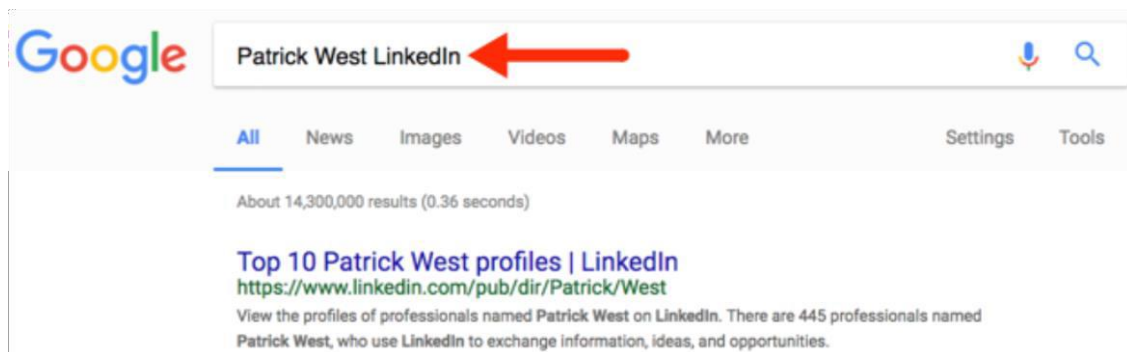
How to find a subject's public profile:

- If you are logged in to your LinkedIn account, you may search for the subject's profile through LinkedIn's search box in the upper left-hand corner of the screen. If you are able to locate the subject and view the subject's profile page, the public profile URL will be identified under the field "Contact Info" under the member's name. LinkedIn members can use settings to control the visibility of certain portions of their profile, such as their profile photo; what you are able to view on a subject's profile may be affected by those visibility settings and your degree of connection to the subject.



LinkedIn Data Request Guidelines

- Alternatively, but only if the member's profile settings permit it, you may search for the subject's LinkedIn profile via an outside search engine such as Google, Bing, etc., when you are not logged in to your LinkedIn account (for example by searching for "John Doe LinkedIn" via Google). Clicking on the link provided at the search engine's site typically directs you to the public profile of the LinkedIn Member, and the public profile URL will appear at the top of your web browser after clicking.



LinkedIn Data Request Guidelines

5. What types of information may be available in response to a Data Request?

Much of the information on LinkedIn is public, and can be found simply by searching on LinkedIn or using a search engine such as Google, Bing, etc. However, depending on the type of formal legal process provided, we may be able to respond with one or more of the following types of data:

Basic Subscriber Information, which may include:

- Email address(es)
- Account URL
- Date and time of account creation
- Billing information
- Address
- Phone Numbers
- IP Logs, which may include:
 - IP address
 - Dates of account log-ins

LinkedIn is only able to provide member content with a valid search warrant from an entity with proper jurisdiction

Member Content may include:

- Invitations
- Messages
- Connections

6. How long does LinkedIn retain Member data?

LinkedIn generally does not retain a copy of information from a Member's profile page once the information has been revised or removed by the Member. Other categories of data relating to Member accounts, such as account log-in history, are subject to automated deletion cycles after a defined retention period. Additionally, in the normal course, when Members close their accounts, we promptly delete or de-personalize the account information, generally within 20 days of account closure.

7. Will LinkedIn notify Members of Requests for account data?

Yes. LinkedIn's policy is to notify Members of Requests for their data unless we are prohibited from doing so by statute or court order. Law enforcement officials who believe that notification would jeopardize an investigation should obtain an appropriate court order or other valid legal process that specifically precludes Member notification, such as an order issued pursuant to 18 U.S.C. §2705(b). When a Request is accompanied by a judge-signed nondisclosure order, LinkedIn will not notify the member before producing the data. However, if the order is overturned or expires on its own terms, LinkedIn may notify the member. Nondisclosure orders should be as narrow in scope and duration as circumstances permit. Note that LinkedIn does not provide advance notice to the Requesting party that a nondisclosure order is expiring; it is up to the Requesting party to calendar the nondisclosure period and to keep LinkedIn apprised of any modifications or extensions.

If your Data Request draws attention to an ongoing violation of our Terms of Service, we may take action to prevent any further abuse in order to protect the network and other LinkedIn Members, including actions that could notify the Member that we are aware of his or her misconduct.

8. Are there any additional requirements for non-U.S. or non-Irish Data Requests?

Yes. At the present time, a Mutual Legal Assistance Treaty (MLAT) Request or letter rogatory is typically required for disclosure of information in connection with a non-U.S. or non-Irish Data Request.

LinkedIn Data Request Guidelines

9. How do I serve a Criminal Data Request on LinkedIn?

A Criminal Data Request may be served by as follows.

1. For all U.S.-based and non-EU-based requests:

By delivering the request in person or via certified mail or express courier to this address:

LinkedIn Corporation
ATTN: Legal Department
1000 West Maude Avenue
Sunnyvale, CA 94085
USA

By sending the request via email to lera_us@linkedin.com.

2. For all EU-based requests:

By delivering the request in person or via certified mail or express courier to this address:

LinkedIn Ireland U.C.
ATTN: Legal Department Wilton
Plaza Wilton Place, Dublin 2
Ireland

By sending the request via email lera_ie@linkedin.com.

10. How do I serve a Civil Data Request on LinkedIn?

In the case of civil subpoenas, LinkedIn will only provide data where the requested information is indispensable to the case, and not within a party's possession. In the normal course, Member data should be sought from the Member directly, who can use automated account tools to download an archive of the relevant data from the LinkedIn Privacy & Settings tab.

Civil requests will not be accepted via email. They must be served upon LinkedIn's agent for service of process. Civil requests for data controlled by LinkedIn Corporation must be domesticated under applicable California procedures for obtaining records from LinkedIn. Civil requests for data controlled by LinkedIn Ireland U.C. must comply with applicable law including European Union regulations on the enforcement of titles.

11. What should I do if I have an Emergency Request for data?

LinkedIn takes significant steps to protect its Members' data, including requiring valid legal process before producing any information about our Members or their accounts. However, we are also aware that certain emergency situations may arise that require the disclosure of Member data. For these purposes, an emergency situation is only one involving imminent and serious bodily harm or death. Where these circumstances are present, Emergency Requests must be made by an authorized law enforcement agent, under penalty of perjury, using the Emergency Disclosure Request Form at the end of the Guidelines. If you are not a law enforcement agent and you are aware of an emergency situation, please notify your local law enforcement officials. LinkedIn will respond to Emergency Requests only if it believes in good faith that serious bodily harm or the death of a person may occur if we do not respond without delay. In all other cases, LinkedIn will disclose information only pursuant to valid legal process that satisfies the requirements set forth above and all applicable legal standards.

LinkedIn® EMERGENCY DISCLOSURE REQUEST FORM

Requesting Agency Name:
Requesting Agent Name:
Requesting Agent Badge/Identification Number:
Requesting Agent Employer-Issued E-mail Address:
Requesting Agent Phone Number (including extension or cell phone):

Detailed description of the nature of the emergency and why the threat is imminent and if applicable a link or screenshot of concerning material on LinkedIn (i.e., description of why there is a potential for imminent serious bodily harm or death and why the normal disclosure process would be insufficient):

Identifying Information for Member account ((1) LinkedIn public profile URL or (2) name and email address):

Detailed explanation of information needed to resolve emergency (Please do not respond by asking for all available information as this will likely result in delaying or denying your Request):

I declare, under penalty of perjury, that to the best of my knowledge, the foregoing is true and correct.

Signature and Badge Number

Date

Name