

Leadership Dismissed who I am, yet they had my results. I was doing what a Specialist does.

September 2025

— colleague Question About Leadership (Captain *without Empathy**)

A colleague was passing by my station and asked if I had experienced more than one issue with “Captain”

I responded yes, sharing that one issue was “Leadership” saying that my packing was wasteful — which bothered me deeply.

It bothered me because I have 15 years of experience in packing and storage, and I’ve always been careful and resourceful in my work.

I felt Leadership was dismissive of my skills and contribution. She listened, and I could see she was weighing her own experiences against mine.

She shared she was considering looking for another job because she felt picked on and unsupported.

I had felt that way myself in a previous workplace, so I understood what she meant, but at the time I didn’t think my own job would be taken from me.

I was responding to how she was feeling, and I told her I was sorry she was feeling that way.

The only advice I could give her was to document everything that happens, the same approach I had been taking myself.

As I saw Leadership in the distance, I said to the colleague that when I had a moment next time, we could talk more, suggesting a break that aligned with hers. She agreed, responding, “Yes, definitely.”



Slack Message and Intimidation

Note: The Slack message and the reassurance conversation with the colleague occurred around the 23rd of September 2025, approximately one month before my dismissal. Due to my revoked access, I cannot confirm the exact date, but this approximation reflects the timing as accurately as possible.

I had been meaning to catch **the same colleague** on her breaks but was just too busy, so I sent her a direct message on Slack.

I wanted her to know I wasn't dismissing her — I was also trying to work around when best to speak with her, preferably when “Leadership” wasn't present. “Leadership” never gave any notification when she took leave, and I commented that my timing was way off, as it appeared “Leadership” may have been absent that week.

The same colleague replied back, saying she understood. Another message followed suggesting that I delete my message to her and she would delete hers. She wasn't being paranoid — she was clearly intimidated, worried that “Leadership” could read our private messages. That fear said everything about the atmosphere we were working in.

I did not want this to be a reason that we could only communicate in passing and only if the timing was right.

Beaver used Slack for communicating and connecting to different departments, and I believed it was a way to connect with colleagues when not all of us had the time to interact in person.

I researched Slack on my own — what it is, how it works, and the different plans — because researching is instinctive for me.

It is something I have always done, and the company already had my specialist profile, so they knew this behaviour was normal and expected.

Even though I didn't know her well, her fear showed how unreasonable and unethical the atmosphere had become. Without warning, my access was revoked immediately upon dismissal.

I am therefore unable to produce the Slack messages directly, but my research was done in my own time, and the messages between a colleague and me are accurate because I retained that information in my own history.



My Research

Monday, Sep 8 🔍 Slack messages

a lady who works at the same place but in a different apartment, seems concerned that the people who are leaders can see their messages on slack, and suggested deleting our conversations so I did . But I would like to know is that false?

It's not entirely false—but it's not quite true either. Here's the real deal:

🔍 Slack messages aren't automatically visible to leaders, but...

- **Workspace Owners and Admins** (which may include certain leaders depending on your company's setup) *can* request access to **private messages and DMs**, especially if your company uses Slack's paid plans govfacts.org suptask.com.
- On **free Slack plans**, they usually need to submit a legal request to Slack to access private messages mozillafoundation.org.
- On **Enterprise Grid plans**, admins may have tools that allow them to export and view messages without needing Slack's help mozillafoundation.org.

So yes, **your employer technically owns the data** in Slack, and under certain conditions, they can access it—even private chats govfacts.org. That said, it's not like managers are casually scrolling through everyone's DMs. It typically requires deliberate action, and often a legal or compliance reason.

If she's worried, it's not a bad instinct to be cautious. But unless your company has a policy of monitoring Slack messages or uses advanced admin tools, it's unlikely that leaders are reading your chats.

Want help checking your workspace's privacy settings? I can walk you through it.

Great question—and the answer depends on **what kind of channel** you create and **what kind of Slack plan** your company uses.

Private vs Public Channels

- **Public channels:** Anyone in the workspace, including leaders, can see and join these. No secrets here.
- **Private channels:** Only invited members can see the channel and its contents. Leaders can't just peek in—unless they're added.

But Here's the Catch...

If your company uses **Slack's Enterprise Grid** or has enabled **compliance exports**, then:

- **Workspace Admins** (which may include leaders) can **access private channel content**, even if they're not members toolingant.com.
- They can also use third-party tools or Slack's own export features to retrieve messages for legal or compliance reasons mozillafoundation.org.

So while creating a private channel gives you some privacy, it's not bulletproof.

Think of it like a locked room in a building your employer owns—they might not have the key, but they can request one if needed.

If you're curious about your workspace's privacy setup, you can check your Slack settings at:

[\[yourworkspace\].slack.com/account/workspace-settings#retention](https://[yourworkspace].slack.com/account/workspace-settings#retention)

Want help interpreting what you find there? I've got your back.

Compliance exports in Slack are a feature that allows Workspace Owners and Admins—especially in larger organizations—to **access and export message data** for legal, regulatory, or internal review purposes. Think of it as a behind-the-scenes tool for companies to stay on top of data governance.

What Compliance Exports Can Include

Depending on the Slack plan, exports may contain:

- **Messages from public channels** (available on all plans)
- **Private channel messages and direct messages (DMs)** (available on Business+ and Enterprise Grid plans)
- **Links to shared files** (not the files themselves unless separately stored)
- **Metadata** like timestamps, user IDs, and message types

These exports are typically delivered in **JSON format**, though Enterprise Grid allows **TXT format** for single-user exports trailhead.salesforce.com.

Who Can Use It?

- On **Free and Pro plans**, only public channel data is accessible.
- On **Business+**, Workspace Owners can apply to Slack for access to private messages and DMs.
- On **Enterprise Grid**, Organization Owners can export **everything**, including private channels and DMs, without needing Slack's approval trailhead.salesforce.com slackalternative.com.

Why It Matters

Compliance exports help organizations:

- Meet legal and regulatory requirements (like GDPR, HIPAA, or CCPA)
- Conduct internal audits or investigations
- Retain records for litigation or HR purposes

Important Caveats

- These exports don't include deleted files.
- They're not visible to regular users—only admins with the right permissions.
- Slack doesn't notify users when their messages are exported.

You can read more in Slack's official guide on [workspace data exports slack.com](https://workspace-data-exports.slack.com) or explore Salesforce's Trailhead module for a deeper dive trailhead.salesforce.com.

If you want help checking whether your workspace has compliance exports enabled, I can walk you through the settings.

Using **compliance exports in Slack** carries several legal implications, especially in the context of **data privacy, workplace investigations, and litigation**. Here's a breakdown of what matters most:

Legal Implications of Compliance Exports

1. Employee Privacy Expectations

- Even though Slack is a workplace tool, employees often assume **private channels and DMs are confidential**.
- Using compliance exports to access these messages can raise **privacy concerns**, especially if employees weren't clearly informed that their messages could be monitored or retrieved.

2. Data Ownership and Custody

- Legally, the **employer owns the Slack data**, not the individual employees.
- This means companies can access and export messages for **internal audits, HR investigations, or legal discovery**, but they must maintain a **clear chain of custody** to ensure the data's integrity [brewminate.com](https://www.brewminate.com).

3. Discovery and Litigation

- Slack messages can be **used as evidence** in lawsuits, especially in employment disputes, harassment claims, or regulatory investigations.
- Legal teams must ensure that exports are **targeted, defensible, and properly preserved** to avoid challenges to their admissibility in court [brewminate.com](https://www.brewminate.com).

4. Regulatory Compliance

- Industries like finance, healthcare, and government may be subject to **strict data retention and monitoring laws** (e.g., HIPAA, GDPR, FINRA).
- Slack compliance exports help meet these obligations, but misuse or overreach can lead to **regulatory penalties**.

5. Transparency and Consent

- In some jurisdictions (like the EU), employers may need to **notify employees** or obtain **consent** before accessing private communications.
 - Failure to do so could violate **data protection laws** and result in legal action.
-

Best Practices to Stay Legally Safe

- **Update internal policies** to clearly state how Slack data may be accessed.
- **Limit exports** to relevant timeframes, users, and channels to avoid unnecessary exposure.
- **Document the process** to maintain defensibility in case of legal review.
- **Use secure tools** to store and analyze exported data, preserving metadata and context [brewminate.com](https://www.brewminate.com).

If your organization is considering using compliance exports, it's wise to consult legal counsel and ensure your policies align with local laws and employee expectations. Want help drafting a sample Slack privacy policy or internal communication notice? I can help with that too.

Absolutely—compliance exports in Slack have played key roles in **real-world legal, regulatory, and internal investigations**. Here are a few illustrative examples that show how they're used:

1. Workplace Misconduct Investigation

A company received a report of **harassment** involving private Slack messages. To investigate, HR and legal teams used compliance exports to retrieve:

- Direct messages between the involved parties
- Private channel conversations
- Timestamps and message metadata

This allowed them to verify claims, take disciplinary action, and document the process for legal defensibility slack.com.

2. Litigation & eDiscovery

In a lawsuit involving **trade secret theft**, Slack messages were subpoenaed as part of discovery. Legal teams created a **targeted export strategy**:

- Focused on specific custodians (employees under investigation)
- Narrowed by date range and topic
- Exported in JSON format for compatibility with eDiscovery tools

This helped reduce costs and ensured only relevant data was reviewed, preserving the chain of custody [brewminate.com](https://www.brewminate.com).

3. Regulatory Compliance in Finance

A financial services firm was required by law to **archive all communications** related to client transactions. Using Slack's **recurring export feature**, they:

- Automatically exported public and private channel messages
- Stored them securely for audit readiness
- Ensured retention policies aligned with FINRA and SEC requirements

This proactive approach helped avoid penalties and maintain transparency trailhead.salesforce.com.

4. GDPR Data Access Request

A former employee in the EU requested a copy of all personal data retained by their employer. Under **GDPR**, the company was obligated to comply. They used Slack's export tools to:

- Retrieve messages from public and private channels
- Include metadata and file links
- Deliver the data in a readable format

This fulfilled the legal requirement and demonstrated responsible data handling slack.com.

These examples show how compliance exports aren't just technical tools—they're legal lifelines when transparency, accountability, and defensibility matter most.

– Slack Research Conversation

Once I felt I had the correct information that was relevant to **the same colleague's** concern, I messaged her:

Johanna to the same colleague:

“Hey [**the same colleague**], just wanted to reach out quickly — I know you were feeling uneasy about Slack DMs not being private. I looked into it properly, and I hope this helps put your mind at ease.

Our company is only on a Slack Pro subscription, and under that plan, management cannot directly access private messages or DMs by default.

They can see public channels and activity dashboards, but they cannot access private DMs or private channels unless they go through a formal process with Slack, providing a valid legal reason. It's not automatic, and it's designed to protect employee privacy.

Also, I checked — there are only three Workspace Admins/Owners:

Clinton (Primary Owner), Josh Beaver (Owner), and Alex (Admin).

They can only export files from public channels, not private ones. I know a few of us have felt uncomfortable, but the reality is more reassuring.

And please know — even if I look serious and move fast, you can always reach out if you need to talk. I'm here.”

The same colleague to Johanna:

“Thanks Jo, so nice of you to look into this and let me know. All good, I know you are busy and the same goes for me also. I am often whizzing through the warehouse to have a smoke and call my bf who is FIFO. He does 8/6 which is pretty good. He flew out this morning. I try not to take too long on my smoko’s as I know others are keeping an eye on my time. My lunch break has been reduced to allow for a morning and afternoon smoko, believe it or not.”

Although my research was sparked by the moment **the same colleague** suggested we both delete our messages, I had also been feeling uneasy for some time.

There was no clear process, rules kept changing, and expectations from leadership were inconsistent.

Response 23 September 2025

Johanna to the same colleague:

Hey [the same colleague], thanks for sharing that — I really appreciate your openness. It’s wild how much pressure we can feel over the smallest things, especially when people in higher positions seem to shift the goalposts or act like we’re doing something wrong. I totally get what you mean — I’ve felt uneasy myself, which is why I went digging into the Slack stuff properly. It’s hard to feel confident when rules keep changing or when experienced people like you (15 years is no joke!) still get nitpicked.

Honestly, I think a lot of us are just trying to do our best while juggling everything — and it’s frustrating when that effort isn’t always seen or respected. You shouldn’t have to feel watched just for taking a breather and checking in with your partner. FIFO life is tough enough without extra stress at work.

Anyway, I’m really glad we had this chat. If you ever want to vent or bounce ideas, I’m here — no judgment, just support.

— Johanna

