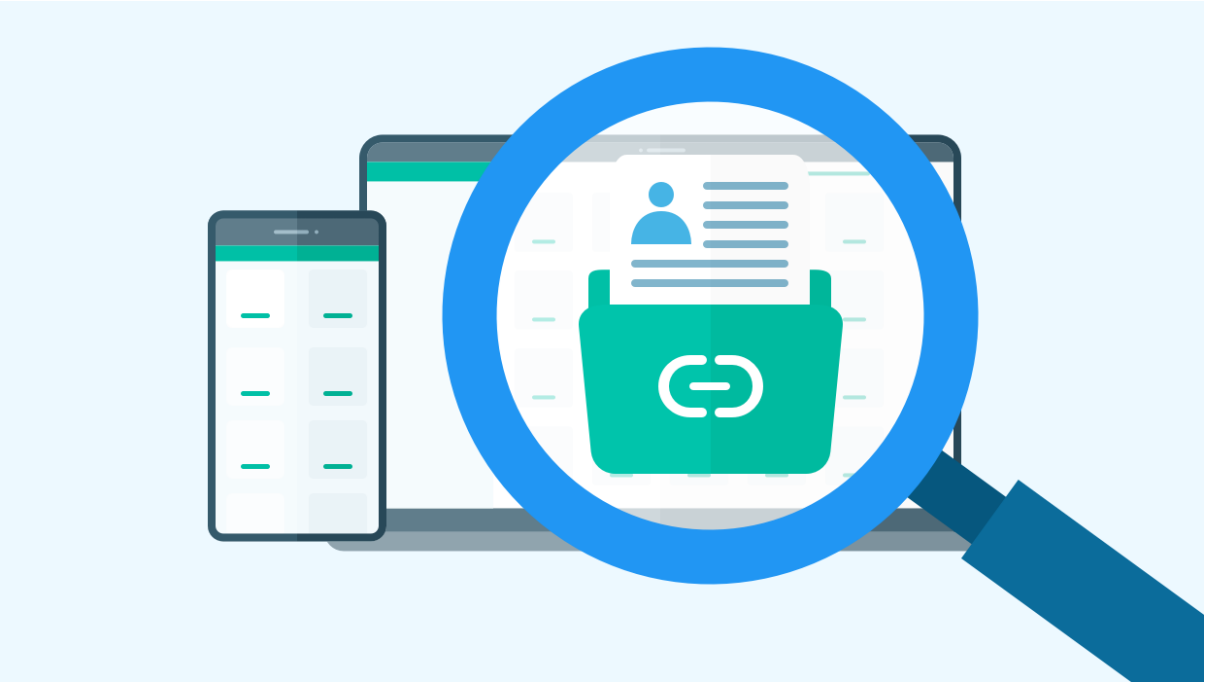

Mega Transparency Report

September 2020

Requests for Removal of Content and for User Information

Report Issued 2 December 2020

Introduction

This is the sixth transparency report published by Mega since it commenced operations in January 2013. Today, Mega has over 200 million registered users in more than 200 countries and territories. In total, Mega's users have stored more than 87 billion files. In accordance with its Privacy & Data Policy, Mega periodically publishes statistics on takedown requests, subscriber information disclosure and related issues.

In 2013, Mega pioneered user-controlled end-to-end encryption through the web browser. It provides the same zero-knowledge security for its cloud storage and chat applications, whether through a web browser, mobile app, desktop app or command line tool. MEGA The Privacy Company provides **Privacy by Design** with zero-knowledge user-controlled end-to-end encryption.

All chat messages and files stored on Mega are fully encrypted on the user's device, using keys encrypted with the user's password. The password remains on the user's device and is never sent to Mega, so chats and file contents can't be read or accessed in any manner by Mega. Files can only be decrypted by the original uploader through a logged-in account or by other parties who have consciously been provided with file/folder keys by the account holder.

Mega stores very limited non-encrypted Personal Data, such as the user's email address and some activity detail relating to account access, file uploads, shares, chats etc. A full description of the information Mega stores about a user and their activities on Mega's system can be found in clause 7.3 of Mega's Privacy & Data Policy.

Regulatory Background

Mega was designed and is operated to ensure that it achieves the highest levels of compliance with regulatory requirements.

Mega's service is governed by New Zealand law and users submit exclusively to the resolution of any disputes by arbitration under New Zealand law. Mega has sought extensive legal advice on its service from lawyers in New Zealand and various other jurisdictions in order to minimise the risk of non-compliance with regulatory requirements in the primary locations in which it operates.

Mega maintains market-leading processes for dealing with users who upload and share copyright infringing material or breach any other legal requirements. Mega cannot view or determine the contents of files stored on its system as files are encrypted by users before they reach Mega. However, if a user voluntarily shares a link (with its decryption key) to a folder or file that they have stored on Mega, then anyone with that link can decrypt and view the folder/file contents. Mega's Terms of Service provide that copyright holders who become aware of public links to their copyright material can contact Mega to have access to the offending files disabled.

By complying with the relevant provisions of New Zealand's Copyright Act, Mega is provided with a safe harbour, shielding it from liability for the material that its users upload and share using Mega's services. Although not technically bound by US or EU law, Mega also complies with the

conditions for safe harbour under the US Digital Millennium Copyright Act (**DMCA**) process and the European Union Directive 2000/31/EC. Mega does this by allowing any person to submit a notice that their copyright material is being incorrectly shared through the Mega platform. When Mega receives such notices, it promptly removes or disables access to the specified file or files, in accordance with Mega's Terms of Service agreed to by every registered user. The number of files which have been subject to such takedown notices continues to be very small, indicative of a user base which appreciates the speed and flexibility of Mega's system for legitimate business and personal use.

The safe harbours in various jurisdictions require material to be removed or links disabled expeditiously. Some cloud storage providers target takedown within 24 hours. Mega targets takedown within a maximum of 4 hours, with most takedowns being actioned within minutes.

When designing and implementing its takedown policy and processes, Mega consulted with New Zealand law enforcement authorities. Mega has adopted policies and processes which it has been advised are consistent with their requirements[1].

Mega has Terms of Service that have to be acknowledged by every new user before their account activation can be completed. Those Terms make it very clear (e.g. in clauses 13.6 and 17-20) that Mega won't tolerate infringement or any other illegal activity.

However, it is impossible for Mega to review content uploaded by users, as it is encrypted at the user's device before it is sent to Mega.

It is also logistically impossible for any cloud storage service (or indeed any other service provider in the Internet chain, such as the connectivity provider, browser supplier, etc.) to review all uploaded content due to the massive volume of data that transits these services. For example, Mega's users upload approximately 65 million files per day, 750 files per second on average. The infeasibility of policing user uploads has been clearly recognised in numerous court cases around the world.

Even if content could be reviewed, in many cases it would not be possible to determine whether it is infringing or not as the owners of many copyrighted materials provide the user with a licence to make a backup copy, so uploading it to a cloud storage service would not be infringing.

Other similar cloud storage services also don't attempt to assess the copyright status of uploaded materials.

[1] https://mega.nz/terms
https://mega.nz/takedown
https://mega.nz/copyright

Requests for Removal of Content

Mega's approach to dealing with requests for the takedown of content uploaded by its users (as well as requests for the disclosure of user information and data) is set out in its Takedown Guidance Policy.

Mega accepts takedown notices via a dedicated web page[2] or by email to copyright@mega.nz Requests are promptly processed without reviewing their validity[3].

The rights holder is able to specify one of three outcomes:

1. Removal of just a specified link to the file: - *the file will remain in the user's account;*
2. Removal of all links to the file: - *the file will remain in the user's account;*
3. Removal of all links to and all instances of the file: - *there is no user permitted to store this file under any circumstance worldwide.*

Folder links often refer to a large number of files, of which only some may be claimed to be infringing files. If the person requesting the takedown doesn't provide identification of the infringing file or files within the folder, Mega will disable the reported folder link as folder contents can change. This means that the folder and its files will remain active in the user's account. This would be the same as option (1) above in respect of file takedown requests.

Mega receives counter-notices from some users who dispute the validity of a takedown. These counter-notices are processed in accordance with safe harbour requirements. Most of the counter-notices Mega receives are genuine and appropriate. This is probably because many content owners and agents trawl the Internet using robots which generate incorrect notices on behalf of copyright owners, and due to the failure of owners and agents to review the specific link content.

The number of unique takedown requests submitted represents a very small percentage of the total number of files stored on Mega. In Q3 2020, the links taken down represented 0.0004% of the 84 billion files uploaded to Mega servers.

		Total Takedown Requests	Taken Down Links / Total Files	Total Files (Billion)
2018	Q4	67,315	0.0001%	52.8
2019	Q1	112,260	0.0002%	56.4
	Q2	118,780	0.0002%	60.0
	Q3	86,498	0.0001%	63.8
	Q4	145,640	0.0002%	68.0
2020	Q1	264,483	0.0004%	72.3
	Q2	471,055	0.0006%	77.6
	Q3	312,588	0.0004%	83.5

[2] https://mega.nz/copyrightnotice

[3] It is impossible to review the validity as the file contents are user–encrypted (unless the user has published or provided the encryption key), and also due to the uncertainties of copyright status as noted above.

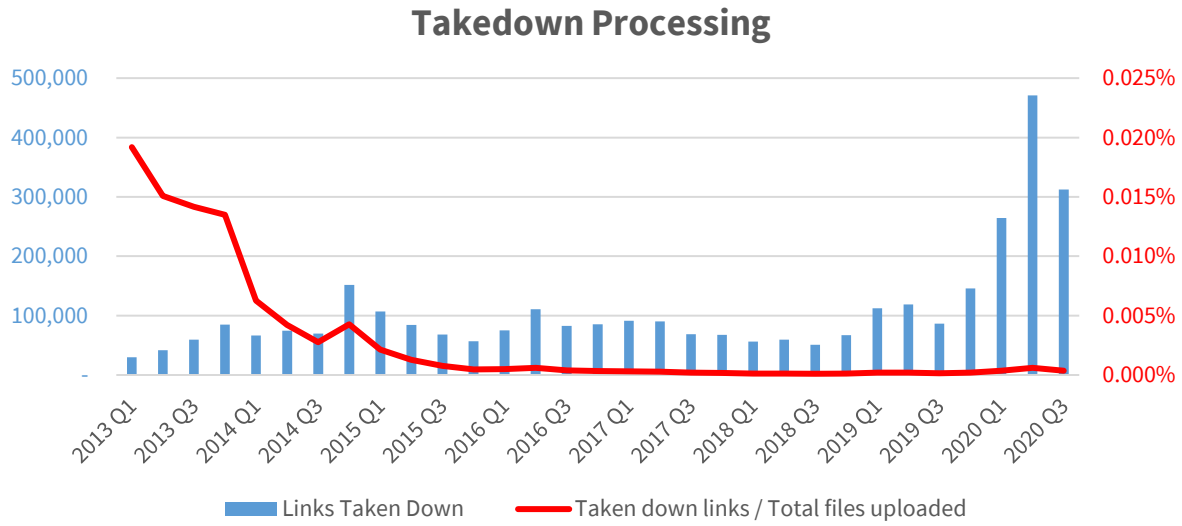

Figure 1 - Requests for file takedowns are a very small % of files uploaded

Repeat Infringers

Mega suspends the account of any user with 3 copyright takedown strikes within six months. In some cases, the account can be reinstated where it is proved to be the subject of invalid takedown notices, but most suspended accounts are terminated. As of 30th September 2020, Mega had suspended 94,966 users for repeated infringement. The data below shows that suspensions have declined to a very small % of the number of registered users.

Year	Quarter	Number of Suspended Users	% of Registered Users
2018	Q4	2,213	0.002%
2019	Q1	2,394	0.002%
	Q2	2,316	0.002%
	Q3	1,462	0.001%
	Q4	1,862	0.001%
2020	Q1	2,047	0.001%
	Q2	3,079	0.002%
	Q3	1,857	0.001%

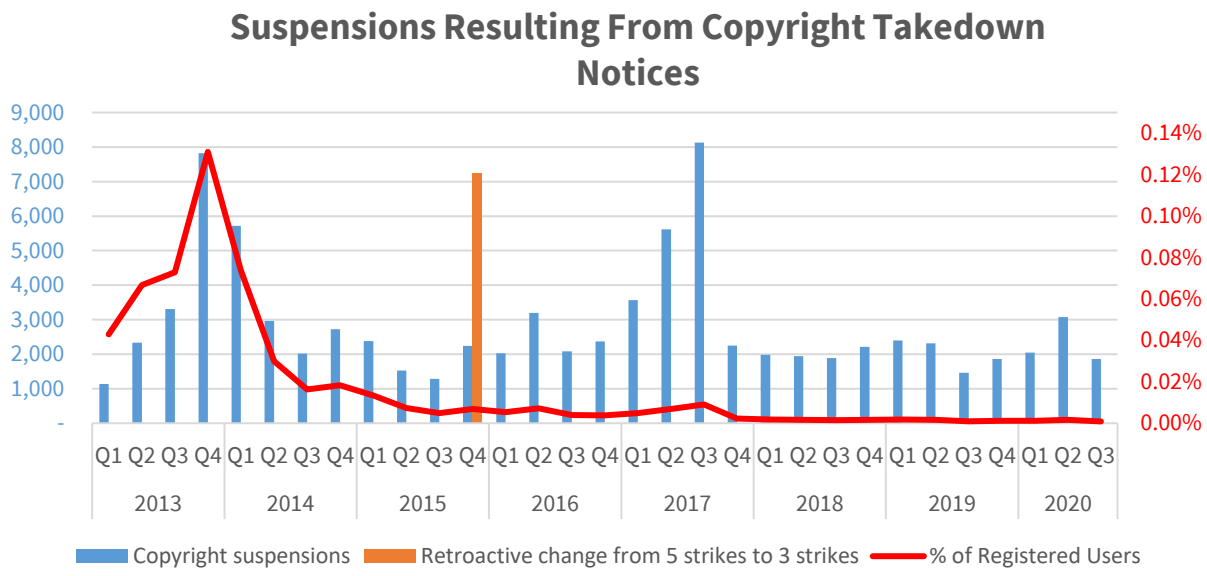

Figure 2 - Copyright Suspensions continue to be a very low % of registered users

Objectionable (Illegal) Content - Child Exploitation Material, Violent Extremism, Bestiality, Zoophilia, Gore, Malware, Hacked/Stolen Data, Passwords

Mega does not condone, authorise, support or facilitate the storage or sharing of Child Exploitation Material (**CEM**), also known as Child Sexual Abuse Material (**CSAM**) or other objectionable material as defined in section 3 of the New Zealand Films, Videos, and Publications Classification Act 1993 or other Internet-harming material. Mega has zero tolerance for users sharing such material. Any reports of such content result in immediate deactivation of the folder/file links, closure of the user's account and providing the details to the New Zealand Government Authorities for investigation and prosecution.

As of 30th September 2020, Mega had closed 565,000 accounts for sharing such content. The account information was made available to the relevant law enforcement agencies.

Appeals against account closure for holding alleged objectionable material are referred to the New Zealand Authorities for adjudication of the content. The account can be reinstated if the content is determined to be not illegal.

Mega is also a strong supporter of the 'Principles to Counter Online Child Sexual Exploitation and Abuse' issued in March 2020[4]. The Principles were produced by a working group of officials from New Zealand, Australia, the United Kingdom, the United States and Canada. Mega was one of the technology companies that provided supportive comment on the draft Principles during the consultation process.

[4] https://www.dia.govt.nz/Voluntary-Principles-to-Counter-Online-Child-Sexual-Exploitation-and-Abuse

Court Orders / Warrants etc

During the year ended 30th September 2020, Mega was served 8 legal orders from NZ authorities and then disclosed account information for the relevant user accounts which are alleged to be involved in serious criminal activity overseas.

Other Requests for Personal Information

Mega is 'The Privacy Company' and values the privacy of its users. We are committed to maintaining industry-leading levels of security for, and confidentiality of, user data and information. In considering any request for access to such data or information, Mega starts from the position that user data and information is private and should always be protected to the greatest extent possible.

However, privacy and protection of user information and data are not absolute rights and are subject to some limitations, such as in cases of illegal activity.

The basis on which Mega may, in extremely limited situations, disclose user information and data is set out in Mega's Takedown Guidance Policy.

Unless an Emergency Response (as defined below) is required, or disclosure is necessary in relation to an investigation involving CSAM or violent extremism, Mega will generally only provide user data or information when required to do so by New Zealand law, or by a New Zealand court or law enforcement authority with appropriate jurisdiction. Mega may consider requests made by non-New Zealand law enforcement authorities.

Mega defines Emergency Response as a situation where Mega has written assurance from a senior officer of the New Zealand Police or similar law enforcement officer or authority acceptable to Mega that in the expert judgment of such person there are valid reasons to believe that disclosure is necessary to prevent or lessen a serious threat (as defined in section 7(1) of the Privacy Act 2020) to:

- public health or public safety; or
- the life or health of an individual or individuals;

and the person giving such assurance confirms in writing that the threat is of such urgency that there is not time to obtain a production order or other court order.

If satisfied as to the above, Mega may, at its discretion, accept the request in good faith.

When Mega accepts a request, Mega will provide advance notice to the affected user unless prohibited by a court order or where Mega decides delayed notice is appropriate, based on criteria described in our Privacy & Data Policy.

Although all files stored on Mega are encrypted prior to being uploaded to our system, and we therefore cannot access that content unless we are provided with the decryption key, Mega does have access to user registration information and the IP addresses used to access our services. A full description of the information Mega can retrieve about a user and their activities on our system can be found in clause 7.3 of our Privacy & Data Policy.

The chart below shows the number of requests for subscriber information that have been processed since 2017.

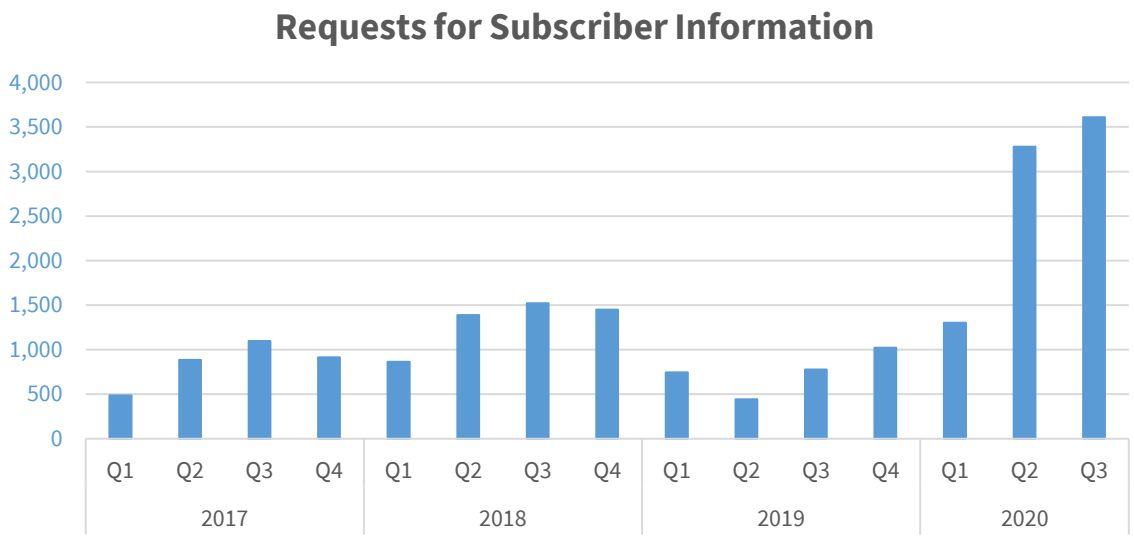

Figure 3 - Requests for Subscriber Information

During the 12 months from 1st October 2019 to 30th September 2020, there were also 7 requests for subscriber information that were declined by Mega, as they did not meet the necessary requirements set out in Mega's Takedown Guidance Policy.

GDPR

The General Data Protection Regulation in Europe came into force in May 2018. Mega didn't need to make any substantial disclosure or make changes to its operations as privacy has been at the core of Mega's operations since it commenced in 2013.

In May 2018, we introduced a feature to allow users to download Personal Data relating to their account. There were quite a few requests in Q4 2018 but the number has reduced significantly since then.

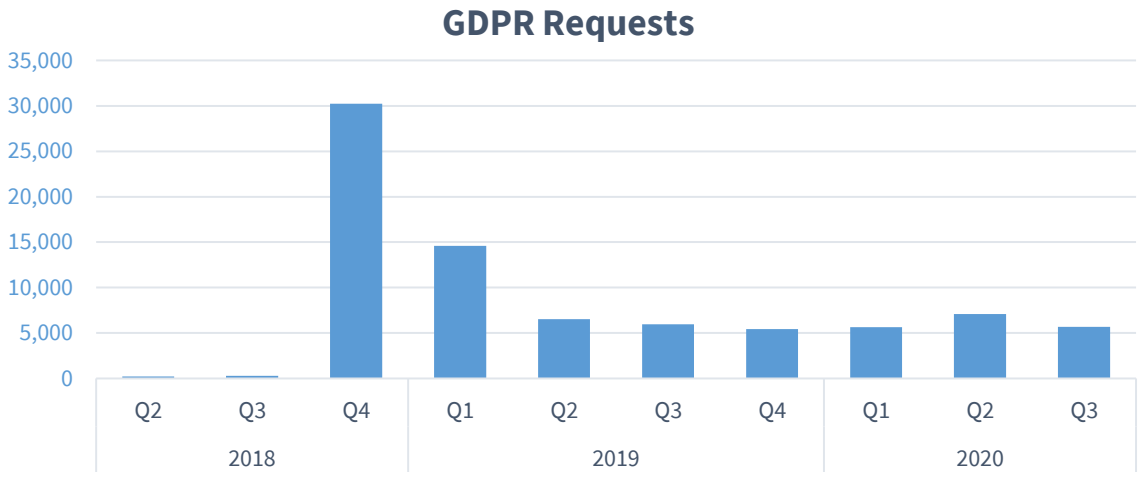

Figure 4 - User downloads of GDPR account information

Personal Data is retained indefinitely while the user's account is open. After account closure, Mega will retain all account information as long as there is any law enforcement request pending, but otherwise for 12 months after account closure, as users sometimes request that an account be re-activated.

After 12 months, identifying information such as email and IP addresses is anonymised (except that email address records are retained for reference by the user's contacts or where the user has participated in chats with other Mega users), but other related database records may be retained. This includes records of financial transactions relating to a user's account where Mega is legally required to retain such information.

When a user deletes a file, that file becomes inaccessible, is marked for deletion and is then deleted fully from the Mega system when the next appropriate file deletion purging process is run.

After account closure, all stored files will be marked for deletion and deleted fully when the next appropriate file deletion purging process is run.

Mega Limited, as controller, is represented in Europe by

Mega Europe sarl
4 Rue Graham Bell
L-3235 Bettembourg
Luxembourg
gdpr@mega.nz

The Lead Data Protection Supervisory Authority is the Luxembourg National Commission for Data Protection. This is the appropriate authority for accepting GDPR complaints about MEGA.

NATIONAL COMMISSION FOR DATA PROTECTION
15, Boulevard du Jazz
L-4370 Belvaux
Luxembourg
https://cnpd.public.lu