28 February 2025

1. Introduction

This Report is published by One.com Group AB ("Group.one") in accordance with the transparency reporting requirements under Article 15 of the European Union's Digital Services Act (Regulation (EU) 2022/2065) ('DSA').

Group.one is a European hosting and SaaS provider, active mainly in the Nordics and DACH regions, Belgium and The Netherlands. In 2024, Group.one provided hosting services in the EU via the following brands: One.com, Hostnet, Antagonist, Zoner, ProISP, SYSE, Uniweb, Dogado, Checkdomain, Easyname, Alfahosting and Profihost.

This report covers the content moderation activities of all the hosting brands mentioned above from February 17th 2024 – December 31st 2024.

2. Orders received from Member States' Authorities (Article 15, 1. (a) DSA)

In the event we receive orders from a Member State authority to act against specific items of alleged illegal content on our platform, we review the reported content in line with our Terms and Conditions and applicable law. If we determine that the content goes against our terms or is illegal, we suspend the specific domain the content was posted on or the entire account of the customer (in case of criminal activity). As the figures show, we are rarely asked to act against illegal content. The vast majority are requests for information in the form of subscriber information.

The statistics below also include notifications which relate to websites where we are not the hosting provider, but only the registrar of the domain name. We do not make the distinction, so we are not able to separate these.

2.1 Member State Orders to act per category

Content category	Orders to act
Consumer Information:Other	0
Illegal or Harmful Speech:Other	1
Intellectual Property Infringements:Other	1
Negative effects on civic discourse or elections	0
Risk for public security	0
Scams and Fraud:Impersonation Account Hijacking	0
Scams and Fraud:Inauthentic Accounts	0
Scams and Fraud: Phishing	0

Scams and Fraud:Other	4
Unsafe and Prohibited Products:Other	1
Violence:Other	0

2.2 Member states orders for information per category

Content category	**Orders for information**
Consumer Information: Other	6
Illegal or Harmful Speech: Other	1
Intellectual Property Infringements: Other	6
Negative effects on Civic Discourse or Elections	3
Risk for Public Security	2
Scams and Fraud: Impersonation Account Hijacking	5
Scams and Fraud: Inauthentic Accounts	84
Scams and fraud: Phishing	2
Scams and Fraud: Other	37
Unsafe and Prohibited Products: Other	2
Violence:Other	1

2.3 Member states orders per country

Member State	**Orders issued**
Belgium	2
Denmark	37
France	7
Germany	100
Hungaria	1
Latvia	1
Malta	1
The Netherlands	4
Poland	1
Spain	1
Sweden	7

2.4 Time to inform the authority of receipt of an Authority Order

We send automated instant responses to confirm the receipt of orders from Member State authorities.

2.5 Median time to give effect to the Authority Order

The median time to give effect to a Member State order for information was **4 days 12 hours**.

The median time to give effect to a Member State order to act was **7 days**.

3. Notices from third parties (Article 15, 1. (b) DSA)

3.1 Number of notices received from third parties by type of illegal content and actions taken

Any individual can notify group.one of illegal or harmful content hosted on our infrastructure. All brands have a dedicated e-mail address where anyone can report illegal or harmful content. As hosting provider, we don't have access to tailored measures like age restrictions or geographical restrictions. The only remedy available to us is suspension of the hosting subscription or domain, which renders the entire website and e-mail of our customers inaccessible (globally).

We review reported content in line with the abuse guidelines published on the brand websites. Our terms prohibit any illegal content. All our sanctions are imposed for violation of our terms and conditions. A lot of notifications we receive are automated notifications from third parties about SPAM and Malware. SPAM or malware can serve an illegal purpose, but that is not necessarily the case. We do not (and cannot) verify in every case whether SPAM or malware is used to conduct illegal activities or not.

Content category	**Notices received**	**Notices actioned (terms and conditions)**
Consumer Information: Other	3	0
Data Protection and Privacy	42	10
Illegal or Harmful Speech: Other	13	1
Intellectual Property Infringements: Other	3 137	1748
Pornography or Sexualized Content	2	0
Scams and Fraud: Impersonation Account Hijacking	294	436
Scams and Fraud: Inauthentic Accounts	715	688
Scams and fraud: Phishing	717	265
Scams and Fraud: Other	6285	4250
Unsafe and Prohibited Products: Other	6	2

3.2 Median time needed for taking action

The Median time needed to take action on reported content after receiving the notification was **4 hours**.

3.3 Notices processed by using automated means Own initiative

All notices are subject to manual review.

4. Own initiative content moderation (Art. 15,1. (c) DSA)

4.1 Information about own initiative content moderation

Group.one does not actively monitor the content that is uploaded by our customers to their web space or domain. We monitor the activity of our customers and suspend in case of suspicious patterns, since this is usually caused by malware. The customer is informed of the suspension due to malware and asked to fix the issue, after which the services are restored. Group.one does not investigate what purpose the malware served.

Besides monitoring suspicious patterns for existing customers, one.com uses a risk engine for new orders. This automated tool scans all incoming orders and assigns them are risk score based on the information entered. Orders above a certain risk score are deemed suspicious are put on a list for manual review. The orders that are deemed fraudulent after manual review are deleted.

4.2 Own initiative statistics

Category	**Amount removed / suspended**
Scams and Fraud: Inauthentic Accounts	20110 (orders removed)
Scams and Fraud: Other	1726 (suspended)

4.3 Measures taken to provide training and assistance to persons in charge of content moderation

The persons in charge of content moderation received an information session on the requirements of the DSA. The employees of the abuse departments are engaged in stakeholder organisations such as the FIT forum (forum mod it-relateret økonomisk kriminalitet), the Internet Infrastructure Forum (an initiative by eco), the Internet & Jurisdiction policy network and M^{3}AAWG (Messaging, Malware, Mobile Anti-Abuse Working Group).

Group.one publishes internal guidelines on content moderation and persons in charge of content moderation can request advice from the legal department on any specific case.

5. Internal complaint handling-handling system (Art. 15, 1. (d) DSA)

The hosting brands of Group.one do not have a formal internal complaint-handling system. Therefore, 0 complaints were received via the internal complaint handling system.