

## WORLDSTREAM DSA TRANSPARENCY REPORT 2024

### 1. Introduction

2024 was a dynamic year for Worldstream B.V. (hereinafter “Worldstream”), marked by continued growth, further professionalisation of its services and an evolving regulatory environment. In this context, the Digital Services Act (DSA) has become an important framework for how Worldstream organises its role as a hosting service provider, in particular with respect to abuse handling, cooperation with authorities and transparency towards stakeholders.

With this report, Worldstream aims to provide clear and reliable insight into how it fulfils its obligations under the DSA and how notice handling, cooperation with authorities and own-initiative measures are embedded in its operations. The underlying figures demonstrate that Worldstream has a mature and well-governed abuse-handling framework, and Worldstream’s ambition is to be among the leading hosting providers in terms of effective, proportionate and transparent DSA implementation. All content-related decisions in 2024 were taken by human staff; no automated tools were used to independently detect and remove illegal content. The detailed figures and breakdowns are presented in the sections that follow.

### 2. Worldstream’s services and role under the DSA

Worldstream operates data centres and network infrastructure, and provides unmanaged infrastructure services, including but not limited to:

1. Dedicated servers and related connectivity services.
2. Colocation services.
3. Network and infrastructure services that enable customers to run their own applications and services.

Worldstream’s role is limited to the technical storage and transmission of information provided by its customers. Worldstream:

1. Does not initiate the transmission of information.
2. Does not select the receiver of the transmission.
3. Does not select or modify the information that is transmitted or stored, except in very limited circumstances such as specific technical support on instruction of the customer, or the execution of lawful orders and abuse measures.

As a result, Worldstream acts as a hosting service provider and intermediary within the meaning of the DSA. Customers retain control over and responsibility for the content and services they deploy on the infrastructure. Worldstream normally has only physical access to hardware, not logical access to customer content. Worldstream benefits from the DSA safe harbour regime, provided it acts expeditiously when it obtains actual knowledge of illegal content or activities and complies with the due diligence obligations applicable to hosting providers, including transparency reporting.

### 3. Legal basis

This DSA Transparency Report for the year 2024 is published by Worldstream in its capacity as a provider of intermediary and hosting services under Regulation (EU) 2022/2065, the DSA. The objective of this report is to provide a clear and comprehensive overview of how Worldstream:

1. Handles orders from competent authorities of EU Member States and, where applicable, from other competent European authorities concerning illegal content and requests for information, as referred to in Articles 9 and 10 DSA and reported under Article 15(1)(a).

2. Operates its notice-and-action mechanism for illegal content, including the handling of notices pursuant to Article 16 DSA, as required by Article 15(1)(b).
3. Applies content moderation and related measures on its own initiative, in particular restrictions on the availability or accessibility of information or on the use of services, as required by Article 15(1)(c).
4. Organises internal complaint-handling mechanisms for users and customers affected by restrictions, in line with Article 15(1)(d).
5. Uses automated means for content moderation and abuse handling, including their purposes and safeguards, as described in Article 15(1)(e).

This report covers the period from 1 January 2024 to 31 December 2024. It is made publicly available at least once per year in an easily accessible, machine-readable format. Worldstream does not operate online platforms or online search engines within the meaning of the DSA. Any dissemination of information to the public occurs through services and applications operated by customers on Worldstream infrastructure, under the customers' control and responsibility. Obligations that only apply to online platforms or to very large online platforms are therefore not in scope of this report.

#### 4. Compliance management and governance

Worldstream maintains a documented compliance framework that integrates legal and regulatory obligations, contractual duties and sector standards. This framework covers, among other topics, the DSA, data protection and privacy rules, sanctions regimes, security requirements and industry codes of conduct.

The following functions are involved in DSA-related compliance:

1. Legal & Compliance  
Responsible for identifying relevant legal requirements, maintaining and updating policies, advising on complex cases and coordinating the DSA compliance framework.
2. Trust & Safety  
Responsible for handling abuse notifications and notices, coordinating Notice and Takedown (NTD) actions, managing interactions with authorities, and overseeing content-related measures that affect the availability or accessibility of information or the use of services.
3. TechCare (Customer Support)  
Responsible for implementing Know Your Customer and Know Your Business procedures, applying sanctions controls, explaining terms and policies to customers and executing decisions that impact customer services.
4. Management  
Responsible for approving policies, ensuring adequate resourcing, and integrating compliance into Worldstream's strategy and operations.

Worldstream follows a principle of service neutrality: it does not conduct general, proactive monitoring of customer content. Content-related decisions are made when there is specific information or notification indicating possible illegality or serious policy breach. Measures are taken with due regard to fundamental rights, including freedom of expression, media pluralism, privacy and data protection.

Policies, internal procedures and training programmes are periodically reviewed and updated, taking into account legal developments, supervisory guidance, enforcement practice and operational lessons learned.

## 5. Know Your Customer and Know Your Business controls

Worldstream has implemented KYC (Know Your Customer) and KYB (Know Your Business) procedures to identify and verify the identity and business profile of customers for the provision of services and, where necessary, throughout the relationship.

Typical KYC/KYB elements include:

1. For natural-person customers: identity details and verification of official identity documents.
2. For legal-entity customers: legal name, registration number, extract from the relevant trade register, business address and contact details.
3. For all customers: billing details and bank account information used for payment.
4. Where required: information about ultimate beneficial owners and control structure.

Worldstream may use external verification and screening services as part of this process. Customer profiles and risk classifications may be reassessed periodically or when specific triggers occur, such as significant changes in ordering patterns, new regulatory developments, signals from abuse handling or authorities' orders, or other risk indicators. These KYC and KYB measures contribute to a safer and more trustworthy infrastructure and support the DSA objective of reducing illegal uses of intermediary services.

## 6. Responsible hosting, codes of conduct, OFFLIMITS and NTD tooling

Worldstream is a member of Dutch Cloud Community and adheres to its Notice and Takedown Code of Conduct. Abuse statistics and serious cases are periodically reviewed at management level to identify trends and opportunities for further strengthening the abuse-handling framework. Worldstream positions itself as a responsible infrastructure provider and a good hoster, in line with relevant sector practices. This includes:

1. Participation in relevant industry associations and adherence to recognised sector codes of conduct, in particular notice-and-takedown codes.
2. Implementation of internal policies such as the Acceptable Use Policy, which prohibits illegal activities and specific forms of misuse (for example, hosting of illegal content, malicious code distribution, large-scale network abuse, spam, unlawful processing of personal data and other abuses).
3. Alignment of internal procedures with the requirements and principles of the DSA, especially regarding notice-and-action, cooperation with authorities and transparency.

Worldstream uses a dedicated Notice and Takedown (NTD) tool that supports:

1. Registration of abuse notifications and notices.
2. Classification by type of alleged illegality or abuse.
3. Assignment and routing to relevant internal teams.
4. Tracking of deadlines, actions taken and resolutions.
5. Reporting and analysis for management and transparency reporting.

Worldstream also supports *OFFLIMITS* and other initiatives that focus on the detection and removal of child sexual abuse material and other serious forms of abuse. This may include cooperation, exchange of non-personal technical indicators and alignment with recommended best practices, in accordance with applicable data protection and confidentiality rules.



## 7. Notice-and-action mechanism (Article 16 DSA)

Worldstream operates a notice-and-action mechanism through which any individual or entity can notify it of allegedly illegal content or activities hosted or facilitated by its services. Publicly available contact channels include a dedicated abuse email address [abuse@worldstream.com](mailto:abuse@worldstream.com) and online forms on the Worldstream website. These channels are monitored by the Trust and Safety team.

Notifiers are requested to provide sufficient information to enable an assessment and possible action, such as:

1. A clear and substantiated explanation of why the content or activity is alleged to be illegal under EU or national law.
2. The category of issue (for example, intellectual property infringement, network abuse, phishing, fraud, CSAM/CSEM, non-consensual intimate imagery, doxxing, privacy violation, other criminal offences or other AUP breaches).
3. The exact technical location of the content or activity, such as URLs, IP addresses, ports, relevant timestamps and system identifiers.
4. Evidence or documentation, where possible (for example, screenshots, log extracts or copies of communications).
5. Contact details of the notifier, unless the nature of the report justifies anonymity, for example in certain CSAM reporting situations.

Upon receipt of a notice, Worldstream:

1. Logs the notice in its NTD ticketing system and assigns a unique reference.
2. Verifies whether the service in question is actually hosted within Worldstream's network or under its control.
3. Assesses whether the notice is sufficiently specific and supported to allow action.
4. Evaluates whether the reported content or activity appears illegal under applicable law or violates Worldstream's Acceptable Use Policy.
5. Considers which measures are technically feasible, necessary and proportionate, taking into account the rights and interests of customers, affected users and third parties.

Where the notice is well-founded, Worldstream may contact the customer responsible for the relevant service, request that the content or activity be removed or changed within a stated period, and, in the absence of adequate action or in urgent cases, impose technical or contractual measures, such as limiting access or suspending services. Worldstream aims to act expeditiously while maintaining a fair, consistent and proportionate approach.

## 8. Statistics on notices (Article 15(1)(b) DSA)

This section presents the statistics required under Article 15(1)(b) DSA regarding notices submitted through Worldstream's notice-and-action mechanism in 2024. In 2024, Worldstream continued to provide infrastructure services that form a core part of many customers' hosting and network environments, with customers hosting key components of their online services and networks within Worldstream facilities and solutions. As a result, Worldstream was frequently identified by third parties as the relevant hosting or network provider and consequently received a substantial number of notices and requests for action which, after verification, related to material or activities outside Worldstream's infrastructure or otherwise beyond Worldstream's technical control.

The figures show that the vast majority of notices relate to alleged copyright or trademark infringement and that a significant portion of notices concern content that is not in fact hosted on, or routed through, Worldstream's infrastructure. All notices were processed manually; no automated systems were used to take decisions on notices.

### 8.1 Overview of notices

In 2024, Worldstream did not receive any notices from trusted flaggers within the meaning of the DSA.

Table 1 – Overview of notices and processing

Metric	Description	Value Format	Total	Trusted Flaggers
Total notices received	The total number of notices submitted through the notice-and-action mechanism regarding allegedly illegal content	Number	27219	0
Total items of information in notices	The number of individual items of content reported in notices. A single notice may cover multiple items	Number	190774	0
Notices processed by automated means	Notices that were fully or partially processed using automated tools	Number	0	0
Median time to act on notices (hours)	The median time between receiving a notice and taking action	Hours	48	N/A

### 8.2 Notices by category of alleged illegal content or abuse

Table 2 – Notices by category and outcome

Category	Number of notices	Percentage of total	Percentage of notices leading to action	Percentage of notices rejected or no action
Copyright or trademark infringement	26477	97.3%	5.3%	94.7%
Network abuse (attacks, scanning, malware)	336	1.2%	19%	81%
Spam and unsolicited communications	115	0.4%	43.5%	56.5%
Web content (non-IP illegal content)	90	0.3%	16.7%	83.3%
Non-Consensual Sexually Explicit Material (NCSEI/NCII)	80	0.3%	38.7%	61.3%
Child Sexual Abuse Material / Child Sexual Exploitation Material (CSAM/CSEM)	79	0.3%	54.4%	45.6%
Unauthorised Personally Identifiable Information (GDPR/Doxxing)	35	0.1%	17.1%	82.9%
Other Acceptable Use Policy Violations	7	0%	0%	100%

This distribution shows that notices about copyright or trademark infringement dominate (over 97% of all notices), while other categories represent only a small fraction of reports.

### 8.3 Main reasons for rejecting or not acting on notices

Table 3 – Main reasons for rejecting notices

Reason for rejection or no action	Number of notices	Percentage of total
Content not hosted on or routed through Worldstream services	20626	75.8%
Insufficient information to identify content or service	2182	8%
Insufficient evidence to substantiate illegality	1058	3.9%
Content or activity not illegal or not in breach of Acceptable Use Policy	1048	3.9%
Content already removed or service already offline	695	2.5%

The high share of notices concerning content not hosted on Worldstream services (75.8%) underlines the importance of accurate identification of service providers in the online ecosystem. The other main reasons listed above account for the majority of remaining cases where no action was taken.

### 8.4 Actions taken on the basis of law versus terms and conditions

Table 4 – Actions taken per legal basis

Action Basis	Count	Percentage
Action based on illegality	1603	99.6%
Action based on terms and conditions	7	0.4%

## 9. Orders from competent authorities (Articles 9, 10 and 15(1)(a) DSA)

Worldstream receives orders from competent authorities in EU Member States and, where applicable, from other competent European authorities, to act against specific illegal content (Article 9 DSA) and to provide information (Article 10 DSA). Orders are received through dedicated authority contact channels and are handled by Trust and Safety in coordination with Legal. Worldstream checks the legal basis and the form and content of orders where possible and acts without undue delay within the scope of the order. Worldstream cooperates with competent authorities in relation to illegal content and information requests. In 2024, Worldstream did not receive any orders to act against specific illegal content under Article 9 DSA, while it received 204 orders to provide information under Article 10 DSA. Of these information orders, 199 were issued by competent authorities in the Netherlands, three by competent authorities in Austria, one by a competent authority in Norway and one by a competent authority in Poland. This section summarises those interactions and the timeframes within which Worldstream responded.

### 9.1 Orders to act against illegal content

Table 5 – Orders to act against illegal content

Metric	Description	Value Format	Value
Total number of orders to act against content	Count of orders from Member State authorities	Number	0
Total number of items of information concerned	Count of individual items referenced in orders	Number	0
Median time to acknowledge orders (hours)	Time to acknowledge receipt	Hours	N/A
Median time to comply with orders (hours)	Time to implement order	Hours	N/A

### 9.2 Orders to provide information

Table 6 – Orders to provide information

Metric	Description	Value Format	Value
Total number of orders to provide information	Count of information orders from authorities	Number	204
Median time to acknowledge orders (hours)	Time to acknowledge receipt	Hours	24
Median time to respond to orders (hours)	Time to provide requested information	Hours	24

## 10. Own-initiative measures and content moderation (Article 15(1)(c) DSA)

Although Worldstream does not conduct general monitoring of customer content, it may intervene on its own initiative when there are clear indications that its infrastructure is being used in ways that are illegal or seriously violate its Acceptable Use Policy, for example in cases of severe network abuse. In 2024, such own-initiative measures were limited in number and focused on disabling services that posed serious security or abuse risks.

Typical triggers for own-initiative measures include:

1. Severe or repeated network abuse detected through technical monitoring, such as large-scale attacks or malware distribution.
2. Persistent patterns of misuse associated with particular services or accounts.
3. Information from trusted partners or authorities indicating serious illegal use of infrastructure.

Possible own-initiative measures include:

1. Temporary blocking or rate-limiting of traffic.
2. Suspension or restriction of specific services.
3. Imposition of technical changes necessary to mitigate ongoing abuse.
4. Termination of services or contracts in severe or repeated cases.

Worldstream seeks to choose measures that are technically workable, proportionate to the risks and respectful of the rights of customers and third parties.

Table 7 – Own-initiative measures

Type of Measure	Total Count	By Automated Means
Content removal	N/A	N/A
Content disabling	17	0
Visibility restriction	N/A	N/A

Own-initiative measures in 2024 concerned disabling or suspending services; there were no separate content removal or visibility-only restriction measures at infrastructure level.

#### 11. Automated tools and supporting systems (Article 15(1)(e) DSA)

Worldstream’s abuse-handling and content-related decisions are primarily made by human staff, supported by internal tools and systems.

Automated or semi-automated mechanisms may be used for:

1. Logging and categorising incoming notices and orders.
2. Prioritising cases based on simple rule sets (for example, known high-risk categories such as CSAM or active network attacks).
3. Correlating cases with existing tickets or known incidents.
4. Reporting and generating aggregated statistics.

Worldstream does not operate large-scale automated content scanning systems on customer content, and automated tools do not independently make final decisions about legality or about restrictive measures. Human review is always involved in decisions which significantly affect the availability, visibility or accessibility of information, or restrict the ability of customers to use services.

Table 8 – Automated detection statistics

Metric	Description	Value Format	Value
Total measures by automated means	Count of all automated actions	Number	0
Total measures without automation	Count of manual actions	Number	1610
Accuracy rate	The percentage of automated measures that were correctly applied	Percentage (%)	N/A
Precision rate	The percentage of items flagged and acted upon by automation that were indeed correctly identified as violating	Percentage (%)	N/A
Recall rate	The percentage of all actually violating items that were successfully identified by automation	Percentage (%)	N/A

The measures reflected in Table 8 relate to actions taken in response to notices under the notice-and-action mechanism; own-initiative measures under Article 15(1)(c) DSA are reported separately in Section 10.

Table 9 – Automated processing of notices under the notice-and-action mechanism

Metric	Description	Value Format	Value
Notices processed by automated means	Notices fully or partially processed using automated tools	Number	0
Notices not processed by automated means	Notices assessed without automated tools (manual review)	Number	27219
Accuracy metrics for automated processing	Precision/recall	Percentage (%)	N/A

In the reporting period, Worldstream did not use automated tools for content moderation in the sense of independent detection and removal of illegal content; all decisions were based on human assessment. As a result, accuracy and error-rate indicators for automated measures are not applicable for the reporting period.

#### 12. Internal complaint handling and user redress (Article 15(1)(d) DSA)

Worldstream provides customers with the opportunity to contest decisions that affect the availability of their content or their ability to use services, where such contestation is legally and practically possible.

Customers can submit complaints through customer support, the abuse contact or account management. Typical complaints concern:

1. Disagreement about whether content or an activity is illegal or in breach of the Acceptable Use Policy.
2. Disagreement about the scope, duration or proportionality of a restrictive measure.
3. Requests for clarification on what is required to restore services or lift restrictions.

These complaint routes form Worldstream’s internal complaint-handling mechanism as referred to in Article 15(1)(d) DSA and in its terms and conditions. Complaints are reviewed by Trust and Safety and, when appropriate, Legal and technical teams. After review, Worldstream may:

1. Confirm the original decision, where it remains justified.
2. Modify the measure (for example, reduce its scope or duration).
3. Fully reverse the decision, where new information or reassessment indicates that it was unjustified or disproportionate.

In 2024, Worldstream handled complaints about content-related and service-restricting decisions through its existing support, abuse and account-management channels. At the time of this first reporting period, Worldstream did not yet systematically register these complaints in a way that allows reliable quantitative reporting of the number of complaints, their basis, outcomes and median resolution times for the full year 2024. As a result, the detailed statistics envisaged by Article 15(1)(d) DSA (for example, counts of complaints leading to confirmation, modification or reversal of decisions) are not yet available for this period.

Worldstream is implementing improved complaint logging and classification in its ticketing and abuse-handling systems. Starting with the transparency report for the 2025 reporting period, Worldstream aims to provide full quantitative statistics on complaints in line with Article 15(1)(d) DSA.

### 13. Zero tolerance for CSAM/CSEM and cooperation with OFFLIMITS

Worldstream applies a strict zero-tolerance policy towards child sexual abuse material (CSAM/CSEM) and related forms of exploitation of minors. CSAM/CSEM is prohibited by law and by Worldstream's policies. Worldstream does not tolerate the presence of CSAM/CSEM and acts against it when it becomes aware of its presence on services operated by Worldstream.

Notifications or indications of CSAM/CSEM are treated as the highest priority and handled with particular urgency and care. Where Worldstream becomes aware that its infrastructure is used for CSAM/CSEM, it will, in accordance with applicable law and internal procedures:

1. Act without undue delay to disable access to the material or services concerned.
2. Preserve or secure relevant information if required for law enforcement investigation, subject to legal constraints.
3. Notify competent authorities or hotlines in accordance with national legal requirements.
4. Terminate customer services or contracts where necessary.

Worldstream supports *OFFLIMITS* and similar initiatives aimed at combating CSAM/CSEM. Where technically and legally feasible, this may include the use of hash lists or other technical indicators, collaboration on best practices and participation in sector-wide efforts to prevent, detect and address CSAM/CSEM.

### 14. Regulatory context and safe harbour regime

The DSA modernises the European regulatory framework for intermediary service providers, including hosting providers, while maintaining a safe harbour regime. Under this regime, hosting providers are not liable for information stored at the request of a user if they have no actual knowledge of illegal content or activities and, upon obtaining such knowledge, act expeditiously to remove or disable access to the information.

The DSA clarifies and complements this regime by introducing due diligence obligations such as:

1. Notice-and-action mechanisms (Article 16).
2. Transparency reporting (Article 15).
3. Statement-of-reasons requirements for restrictions (Article 17).
4. Obligations to notify authorities in case of suspected serious criminal offences (Article 18).

Worldstream has integrated these obligations into its policies and processes, particularly in the fields of notice handling, abuse and security procedures, cooperation with authorities and transparency reporting.

### 15. Overview of Article 15(1) coverage

For ease of reference, the coverage of Article 15(1) DSA requirements in this report is summarised below:

1. Article 15(1)(a) – Orders from competent authorities  
Covered in Section 9, including Tables 5 and 6.
2. Article 15(1)(b) – Notices submitted under Article 16 DSA  
Covered in Sections 7 and 8, including Tables 1, 2, 3 and 4.
3. Article 15(1)(c) – Content moderation on the provider's own initiative  
Covered in Section 10, including Table 7.
4. Article 15(1)(d) – Internal complaint-handling mechanisms  
Covered in Section 12.
5. Article 15(1)(e) – Automated tools for content moderation  
Covered in Section 11, including Tables 8 and 9.



#### **16. Outlook and continuous improvement**

Worldstream will review and update its DSA transparency reporting on an annual basis. As data collection and tooling mature, Worldstream aims to further refine its statistics, in particular regarding complaint tracking and qualitative indicators on the effectiveness of its abuse-handling measures. Worldstream will continue to align its practices with guidance from regulators, industry codes of conduct and initiatives such as *OFFLIMITS*, with the objective of maintaining a safe, resilient and rights-respecting infrastructure environment. These reviews are used to adjust procedures, tooling and training, ensuring that abuse handling keeps pace with evolving threats and regulatory expectations.