Whaleco Technology Limited

Risk Assessment and Mitigation Report

2025

TABLE OF CONTENTS

I. Executive Summary

Whaleco Technology Limited ("**Whaleco**"), incorporated in Ireland, has been operating Temu, an online marketplace, in the European Union ("**EU**") since April 2023. Through the www.temu.com website and the Temu-branded mobile application (collectively, "**Temu**"), Whaleco connects EU consumers ("**consumers**") with third-party sellers ("**traders**") within and beyond the EU, enabling Temu's users to sell and purchase a diverse selection of affordable, quality products. Whaleco places the highest priority on ensuring a reliable, safe and trustworthy environment for EU consumers. In line with the Charter of Fundamental Rights of the EU, Whaleco continuously refines its policies and practices to safeguard consumer confidence, both in individual purchases and their interactions with Temu.

Whaleco conducts annual risk assessments pursuant to Articles 34 and 35 of the Regulation (EU) 2022/2065 (the Digital Services Act, or "**DSA**"), following Whaleco's designation as a Very Large Online platform ("**VLOP**") under Article 33 of the DSA on 31 May 2024.

This year—2025—is another year of growth for Whaleco in the EU, with Temu now supporting a larger and more diverse community of traders and EU users engaging in sales of a broad spectrum of products. The expansion has created challenges as Whaleco navigates the increasingly complex risk landscape. Whaleco recognises that if its risk management capabilities do not evolve in pace with market growth, significant systemic risks could emerge. Such risks include the sale of unsafe products, proliferation of counterfeit products, transactional fraud, and potential impact on users' mental well-being. Annual risk assessments enable Whaleco to maintain current awareness of its risk profile and, in response, to develop and implement tailored controls.

This report ("**Report**") summarises the results of Whaleco's annual risk assessment for 2025 ("**Year 2 risk assessment**"). This year's assessment adopts an evolved methodology building on Whaleco's Year 1 risk assessment. The assessment is grounded in analyses of how Temu's specific features and services, or the use of them by Temu's traders or users, could give rise to inherent systemic risks. In addition, Whaleco employs both quantitative metrics and qualitative analyses from internal and external sources to evaluate the inherent systemic risks stemming from Temu's risk profile, the design and effectiveness of Temu's mitigation controls, and the resulting residual risks remaining on Temu.

The Year 2 risk assessment operates within Whaleco's risk governance framework, which encompasses Whaleco's Board of Directors, the DSA Compliance Function, Delegated Decision Makers ("**DDMs**"), the Legal & Compliance Team ("**LCT**"), and the Trust & Safety Team ("**TST**"). The assessment draws on inputs from internal risk owners and subject matter experts gathered through more than 40 collaborative workshops, as well as findings from external stakeholder engagement with organisations including Safe Non-Food Consumer Products in the EU and China ("**SPEAC**"), International AntiCounterfeiting Coalition ("**IACC**"), and European Consumer Protection Cooperation Network ("**CPC**").

Whaleco divides the Year 2 risk assessment into five modules and seven sub-modules, ensuring full coverage of the four risk categories under Article 34(1) of the DSA:

- **Illegal content**, including (1) Product Compliance, (2) Products infringing intellectual property rights ("**IP**"), and (3) Content Compliance
- **Consumer protection**, including potential negative consequences to EU consumers' economic rights and well-being
- **Protection of minors**, including the potential exploitation of vulnerabilities of minors
- Potential negative effects on the exercise of other **fundamental rights**
- Potential negative effects on **civic discourse and electoral processes**

Below is an overview of Whaleco's risk assessment results. Whaleco assessed inherent and residual risks using a six-tier scale from **High (5/5)** to **Negligible (0/5)**. Control strength was evaluated on a five-tier scale from **Highly Effective (5/5)** to **Not Effective (1/5)**.

- Whaleco assessed the inherent systemic risks for **Illegal Content** as **High (5/5)** because Temu's nature as an online marketplace hosting millions of products gives rise to significant systemic risks regarding illegal content. To address this, Whaleco has implemented a suite of control measures, assessed as **Mostly Effective (4/5)**, including enhanced trader onboarding controls, optimised automated and human content moderation, and systematic integration of external stakeholder feedback. Consequently, the residual risk was assessed as **Medium (3/5)**.

- Whaleco assessed the inherent systemic risks to **Consumer Protection** as **Medium-High (4/5)** given Temu's large EU user base whose economic interests or mental well-being could be exploited by malicious actors. In response, Whaleco enhanced Temu's user interface by enhancing transparency disclosures and removing certain features. In addition, Whaleco implemented mitigation measures, assessed as **Somewhat Effective (3/5**), including stricter controls against fake or duplicate trader accounts and active moderation of product descriptions and trader-user communications. As a result, the residual risk was assessed as **Medium (3/5)**.

- Whaleco assessed the inherent systemic risks to the **Protection of Minors** as **Medium-High (4/5)**. While Temu is not designed for minors and its transactional interactions typically require access to financial resources, Whaleco recognised that minors may still be exposed and remain vulnerable. Whaleco implemented safeguards, assessed as **Somewhat Effective (3/5**), such as parental controls for minors' accounts and age-gating for adult-only products. The residual risk was assessed as **Medium (3/5)**.

- Whaleco assessed the inherent systemic risks to other **Fundamental Rights** as **Low-Medium (2/5)**. While Temu is an online marketplace not designed for political or social expression, indirect systemic risks may arise, such as discrimination, interference with the right to conduct a business, and risks related to privacy and data. Whaleco's corresponding mitigation measures inclu de fundamental rights safeguards in trader policies, fair and transparent search and recommender systems, GDPR-aligned privacy protection, and effective redress via accessible appeals and complaint channels. Measures were assessed as **Mostly Effective (4/5)**. Consequently, the residual risk was assessed as **Low (1/5)**.

- Whaleco assessed the inherent systemic risks for **Civic Discourse and Electoral Process** as **Negligible (0/5)** because Temu, as an online marketplace, does not provide a forum for civic discourse about electoral processes or other political issues.

Whaleco recognises risk assessments as a learning process that informs risk management plans for the upcoming year. Accordingly, Whaleco has identified areas for enhancing its existing mitigation framework, including (1) expanding partnership with accredited organisations to implement systematic product sampling programmes that evaluate and address product compliance and IP risks, (2) strengthening product safety controls by including stricter requirements for labelling and other regulated parameters, (3) leveraging the newly launched Transparency Center as the hub for enhanced disclosures with regard to consumer rights and governance developments, and (4) exploring enhanced age-verification solutions for age-gating products.

II. Introduction

A. About this Report

This Report summarises the results of Whaleco's Year 2 risk assessment conducted pursuant to Articles 33, 34 and 35 of the DSA, following Whaleco's designation as a VLOP under Article 33 of the DSA on 31 May 2024. The Year 2 risk assessment covers data **available between 1 July 2024 and 30 June 2025** (the "**Relevant Period**"), providing sufficient coverage of Year 2 for data extraction, processing, and analysis.

This Report underscores Whaleco's commitment to identifying and mitigating systemic risks stemming from Temu's service designs, features, and operations in the EU, as well as the use made of Temu's services, ensuring Temu remains a safe, trustworthy marketplace for EU users. While Temu operates as a global online marketplace, this Report assesses systemic risks stemming from Temu's EU services that affect the EU community.

B. Assessment Methodology

This year, Whaleco adopted a risk assessment methodology that (1) incorporated feedback from external stakeholders, including the European Commission, Member State enforcement authorities, consumer groups, and civil society; 2) examined the evolving regulatory landscape of emerging laws and regulations; and 3) referenced recognised industry standards, including ISO 31000: Risk Management and ISO/IEC 25389: Information technology - The safe framework. **Section III: Assessment Methodology** outlines Whaleco's Year 2 risk assessment approach.

C. Overview of Temu's Key Attributes

The Year 2 risk assessment is grounded in a structured analysis of Temu's evolving functionalities and services, which Whaleco referred to as "**Temu attributes**". Whaleco identified these attributes and tracked their developments by examining trader and user journeys, including an analysis of Temu's features and services to facilitate and promote sales, such as Temu's terms and conditions, recommender systems, and the Affiliate & Influencer Programme ("**A&I Programme**"). The exercise specifically ensured coverage of the influencing factors outlined in Article 34(2) of the DSA.

Section IV: Overview of Key Temu Attributes identifies the key Temu attributes that may contribute to or influence systemic risks across the various risk categories. This section serves as the primary reference point for factual details about Temu's attributes, thereby reducing redundancy in risk module assessments (**Sections VI to IX**). The modules may, however, include additional attribute details where these are specifically relevant to the risk under discussion.

D. Temu's Risk Governance Framework

Temu operates in a dynamic and rapidly evolving risk environment. The most significant challenges are inherent to the nature of e-commerce, which include the potential listing of and sale of unsafe, inauthentic, or otherwise illegal products. Additionally, Whaleco actively monitors and manages transactional risks, including payment fraud and scams.

To systematically address the risks, Whaleco has developed a suite of mitigation measures that can be classified into six control groups, including 1) a governance, risk & compliance oversight structure ("**GRC**"), 2) policies and standards, 3) user management & onboarding compliance, 4) detection & enforcement, 5) user rights & redress mechanisms, and 6) external engagement. This integrated system ensures Temu's reliability, safety, and trustworthiness for consumer transactions. The

framework addresses both proactive and reactive mitigation measures, ensuring risk mitigation across all identified risk categories. More details are included in **Section V: Temu's Risk Governance Framework**.

E. Risk Module Assessments

The **risk module assessments from Sections VI to IX** encompass four distinct modules mapped to the risk categories under Article 34(1) of the DSA: illegal content, which includes product compliance, IP, and content compliance (**Section VI**), consumer protection (**Section VII**), protection of minors (**Section VIII**), and fundamental rights (**Section IX**).

Pursuant to Article 34(1)(c) of the DSA, Whaleco also assessed potential negative effects on **civic discourse, electoral processes, and public security**.

Whaleco assessed the inherent systemic risk of negative impact on civic discourse and electoral processes as negligible because Temu operates as an online marketplace rather than a platform for political discourse. Temu's product review function, which is the only venue for consumers to post user-generated content, is designed specifically for consumers to share feedback about products they have bought, rather than sharing political views. Although certain traders may attempt to list politically themed products, these items typically contain minimal political messaging that lacks the scope or scale necessary to meaningfully disrupt civic discourse or influence electoral processes. Whaleco's observation on Temu is consistent with relevant disclosures made by other VLOPs operating online marketplaces, indicating that the lack of historical occurrences observed on Temu is not due to a gap in risk identification but rather to common characteristics shared by online marketplaces.

Public security risks on Temu primarily manifest in the form of products and reviews with terrorist elements. As such, this risk will be analysed through the assessment of risks related to illegal content (**Section VI**).

III. Assessment Methodology

Whaleco acknowledges the importance of identifying and addressing risks that may arise on Temu and impact EU consumers and the broader EU economy. Whaleco's Year 2 risk assessment methodology was developed in accordance with the DSA requirements and incorporated feedback from the Directorate-General for Communication Networks, Content and Technology ("**DG Connect**") of the European Commission on Whaleco's previous risk assessment exercises, ensuring alignment with regulatory expectations. The assessment framework also adheres to recognised industry standards, including ISO 31000: Risk Management and ISO/IEC 25389: Information technology - The safe framework.

The following sections provide more details on Whaleco's Year 2 risk assessment methodology, including A. an overview of Whaleco's information sources for the risk assessment and B. the six-step process Whaleco undertook to arrive at the findings presented in this Report.

A. Overview of Input Sources

Whaleco's risk assessment process relied on both qualitative and quantitative inputs, drawing from the following internal and external sources.

- **Structured workshops and fact-finding**: Whaleco conducted over 40 collaborative workshops with more than 110 internal subject matter experts (e.g., Trust & Safety, Marketing, and Customer Service) and external advisors to facilitate fact-finding on Temu features and scenarios and identify those that may influence systemic risks. Assessment results were reflected in iterative probing questions and responses.

- **Data metrics from internal controls and external feedback**: Whaleco's qualitative queries were complemented by quantitative metrics extracted from internal controls, providing insights into the magnitude of Temu's inherent systemic risks and the effectiveness of Whaleco's corresponding mitigation measures.

- **Stakeholder engagement**: Whaleco has maintained engagement with EU and Member State regulators, consumer organisations, and broader civil society to develop an in-depth understanding of the interests and concerns shared by Whaleco's external stakeholders and to incorporate lessons learned into Whaleco's daily risk governance efforts. This approach produces well-supported risk evaluations that reflect both operational realities and stakeholder perspectives. For example:

    - Whaleco engages with European think tanks such as the Centre on Regulation in Europe (CERRE). Through collaborative research programmes, Whaleco seeks to better understand the principles and long-term vision behind digital legislation and to explore how Whaleco can best contribute to a stable and thriving digital economy.

    - Whaleco launched a long-term cooperation programme with Centro per i Diritti del Cittadino (CODICI), a consumer protection organisation in Italy. The five-year cooperation features joint monitoring programmes and annual review meetings designed to drive stronger product compliance measures on Temu.

- **Industry benchmarking**: Whaleco benchmarked risk assessment reports published by other VLOPs operating online marketplaces, and incorporated best practices for assessment methodology, functionality mapping, and risk categorisation. In addition, Whaleco analysed risk occurrences flagged by the European Commission and conducted a scan of publicly available

risks identified by civil society, consumer protection organisations, intergovernmental organisations ("**IGOs**"), and media to discover any recurring or new areas of risk for online marketplace platforms. Whaleco assessed whether these recurring and new areas of risk were also applicable to Temu.

- **External professional advice**: Whaleco engaged an industry-leading Trust & Safety technical advisor with deep experience in DSA risk assessments to guide the formulation of its assessment methodology and the quantitative measurement of key risk indicators. Whaleco engaged prominent legal counsel with specialised expertise in the DSA to advise on qualitative fact-finding and report preparation.

B. Overview of Assessment Process

Whaleco views DSA risk assessments as a continuous process rather than a static annual reporting exercise. Therefore, its assessment process operates as an iterative cycle that drives enhanced understanding of Temu's evolving risk profile and improvement of corresponding controls. The following outlines the six steps Whaleco undertook to complete its Year 2 risk assessment cycle:

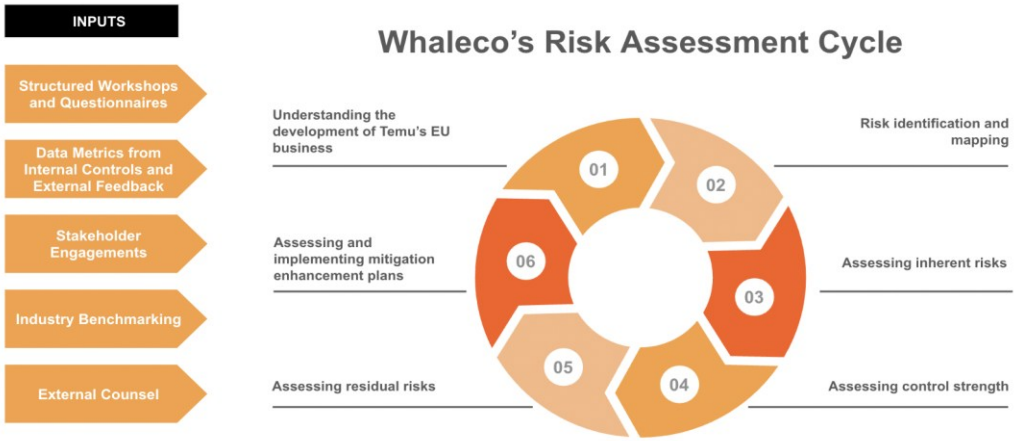


Figure 1: Whaleco's Risk Assessment Cycle

- **Understanding the development of Temu's EU business:** The risk assessment cycle began with an evaluation of the evolutions of Temu's EU business during the Relevant Period, including the development of Temu's existing functionalities, features, and services (i.e., Temu attributes), the introduction of any new Temu attributes, as well as the use made of these attributes by Temu traders and users.

- **Risk identification and mapping:** Following the evaluation of Temu's EU business, Whaleco mapped DSA-related risk types that could potentially be relevant to Temu, ensuring comprehensive coverage of the DSA's list of systemic risks. Whaleco then assessed the relevance of each identified risk type to the risk modules it developed for internal risk management.

- **Assessing inherent systemic risks:** Building on Whaleco's understanding of Temu attributes and the potentially relevant risk types, Whaleco performed an analysis of how each Temu attribute can influence and/or amplify systemic risks. The analysis was complemented by a data-driven risk scoring exercise that gauged the overall probability and severity of the inherent systemic risks stemming from Temu's design.

- **Assessing control strength:** Whaleco then mapped the existing mitigation measures in place against the identified inherent systemic risks and evaluated the effectiveness of these mitigation measures across three dimensions: design quality, operational effectiveness, and mitigation effectiveness as measured by key risk indicators.

- **Assessing residual risks:** Residual risk was determined by the inherent systemic risk level and the effectiveness of mitigation measures in reducing inherent systemic risk. Whaleco employed a matrix framework that evaluates inherent systemic risk against mitigation effectiveness to calculate residual risk levels. In evaluating residual risk associated with illegal content, particularly in the context of product compliance, Whaleco integrated third-party evaluation and testing results to independently verify and validate the assessments derived from its internal data.

- **Identifying and implementing mitigation enhancement plans:** When the risk assessment identified residual risks in specific modules, Whaleco developed targeted mitigation plans to address and manage these risks going forward.

Whaleco explains each of the steps below in further detail.

Step 1: Understanding Temu's EU Business

Article 34 of the DSA requires a VLOP to diligently identify, analyse and assess any systemic risks in the EU stemming from the "design or functioning of their service and its related systems, including algorithmic systems, or from the use made of their services". The first step of Whaleco's risk assessment was to map the designs, functionalities, and services Temu has to offer.

Whaleco recognises Temu as (1) an online marketplace, (2) hosting global traders, (3) who sell products, (4) to EU consumers. These four elements constitute Temu's "core characteristics" that define Temu's fundamental risk landscape.

In addition to the core characteristics, Temu offers a variety of "features and services" that facilitate and promote product sales. Whaleco simulated the journeys of its traders and consumers on Temu to identify existing facilitation infrastructure and promotional features that could influence systemic risks. The results were cross-checked with features and services identified by peer online marketplaces, as well as areas of concern identified by the European Commission. Finally, Whaleco took into account the influencing factors outlined in Article 34(2) of the DSA.

Core Characteristics	Hosting traders
	Hosting product listings
	Accommodating EU consumers
	Distance sales in an online marketplace
Features and Services	Product reviews by consumers
	Limited chat functions
	Report and appealing systems
	Customer services
	Logistics
	Payments
	On-platform promotions
	Off-platform promotions
DSA Article 34(2) Influencing Factors	Recommender systems and relevant algorithmic systems
	Content moderation systems
	Terms and conditions and their enforcement
	On-platform advertisements (not available in the EU)
	Data-related practices

Figure 2: Identified Temu Attributes

Step 2: Risk Identification and Mapping

An essential part of the risk assessment obligation mandated by Article 34 of the DSA is mapping risk types that could potentially materialise on Temu.

Whaleco's risk identification exercise was guided by EU laws and regulations, including (1) Article 34(1) of the DSA and relevant recitals 12, 79, 80, 81, 82, 83, and 84, (2) the Charter of Fundamental Rights of the EU, and (3) other EU regulations and directives, such as the General Product Safety Regulation (EU) 2023/988 ("**GPSR**"), the Consumer Rights Directive (Directive 2011/83/EU), and the Unfair Commercial Practices Directive (Directive 2005/29/EC). The exercise was complemented by a review of enforcement actions by the European Commission against online marketplaces, as well as publications from civil society, consumer protection organisations, IGOs, and media such as the Transatlantic Consumer Dialogue, UN Trade and Development, and the Organisation for Economic Co-operation and Development (OECD).

Whaleco then determined the potential relevance of each identified risk type to the seven risk modules. Risk types potentially relevant to multiple modules were assigned to a primary module under which the risk assessment was conducted. The other risk modules assessed that risk type only where there were unique risk implications for which an additional set of mitigation measures was warranted. For example, prohibited products are by definition illegal content and have negative consequences for consumers' well-being, which is a fundamental right to a high-level consumer protection enshrined in Article 38 of the Charter of Fundamental Rights of the EU. Whaleco mapped prohibited products to the "product compliance" module for primary assessment; other modules assessed prohibited products to the extent they were relevant to the respective risk topics.

	Product Compliance	IP	Content Compliance	Consumer Protection	Minor Protection	Fundamental Rights	Civic discourse/electoral processes
Prohibited products	●			○	○	○	○
Restricted products	●			○	○	○	○
IP infringement	○	●		○	○	○	
Misinformation	○		●	○	○	○	○
Sharing private images	○	○	●	○	○	○	
Exploitation, trafficking, and forced labour	○		●	○		○	○
Terrorist content and other public security risks	○		●	○	○	○	○
Scam & fraud			○	●	○	○	○
Dark pattern and misleading practices				●	○	○	
Transparency & Disclosure	○	○	○	●	○	○	
Consumer rights				●	○	○	
Designs simulating addictive behaviour				●	○	○	
Child sexual abuse material (CSAM)	○		○	○	●	○	○
Exploitation of minor weaknesses	○		○	○	●	○	
Right to privacy			○	○		●	○
Right to dignity			○	○	○	●	
Discrimination and hate speech	○		○	○	○	●	○
Right to free expression and conducting business	○	○	○	○		●	○
Risks to civic discourse and electoral process	○		○	○		○	●

● Primary assessment module ○ Other relevant modules

Figure 3: Risk Identification and Mapping Results

Step 3: Assessing Inherent Systemic Risks

Inherent systemic risks on Temu refer to those stemming from Temu's intrinsic designs, functionalities, and services, i.e., "**Temu attributes**", in the absence of mitigation measures. Pursuant to Article 34(1) of the DSA, Whaleco assessed its inherent systemic risks, qualitatively and quantitatively, from two dimensions: (1) probability, meaning the likelihood that a risk could materialise on Temu in the absence of mitigation controls, assessed primarily by historical occurrences observed on Temu through proactive and reactive monitoring, and (2) severity, meaning the impact of the risk if it were to materialise, assessed from three aspects in accordance with the following UN Guiding Principles:

- **Scope**: the number of users and non-users that are or could be affected
- **Scale**: the nature of the harm (e.g., physical, psychological, economic) and its potential impact on vulnerable groups
- **Remediability**: the platform's ability to restore affected individuals to their state prior to risk occurrences.

Whaleco's inherent systemic risk assessment is a two-step process that begins with 1) developing an internal qualitative understanding and 2) establishing a data-driven foundation, which is then cross-checked against external information.

i. Qualitative analysis of inherent systemic risks

Assessment of inherent systemic risks began with a qualitative analysis of whether and to what extent each Temu attribute identified in Step 1 could impact the probability or severity of the systemic risks identified in Step 2. The analysis incorporated fact-finding results from consultations and workshops with internal subject matter experts. Whaleco also analysed influencing factors that could amplify the dissemination of the risk, as well as potential manipulation or exploitation of Temu services by traders, users, or third parties that could influence the inherent systemic risk level. The fact-finding results were reviewed by Whaleco's external Trust & Safety advisor and legal counsel.

ii. Quantitative assessment of inherent systemic risks

Initial assessment from internal analyses and data: Whaleco first conducted an initial assessment of the likely inherent probability using Temu-specific data, including proactive and reactive metrics. Where metrics were less readily available, such as for inherent severity, Whaleco's assessment was qualitative, consistent with market approaches. This step provides a detailed understanding of the risks directly observable on Temu.

External validation and upward adjustment: This initial score was then validated against external data sources such as peer transparency reports, European Commission regulatory actions, and third-party research. If it indicated a higher risk level, Whaleco adjusted the score upward to reflect the broader market context and potential for unknown or emerging risks. This two-step methodology ensured that the final risk score was not only based on Whaleco's own data, but was also independently validated and, if necessary, strengthened by external signals. This approach prevents potential underestimation of risks.

- **Probability score for inherent systemic risks**: Whaleco determined the probability of inherent systemic risks by considering the frequency of risk occurrences captured in Temu's proactive and reactive metrics. As an additional step, Whaleco validated these findings against external transparency reports from other VLOPs operating online marketplaces and third-party research publications. This conservative approach ensured that low internal incident rates were not taken at face value but were instead cross-checked against broader market-wide patterns. The combination of internal data with external information produced a more reliable, industry-aligned assessment of probability. Following this methodology, Whaleco developed the scoring chart below for the probability of inherent systemic risks along with explanations for each scoring threshold (Figure 5).

- **Severity score for inherent systemic risks**: The severity score is the unweighted average of the scores for scope, scale, and remediability. Whaleco assessed the scope score by considering the number and percentage of EU users and non-users that could be affected by the potential materialisation of the inherent systemic risks. Whaleco assessed the scale score by examining the potential financial, physical, and/or mental harm that the inherent systemic risks could cause if they were to materialise. Whaleco assessed the remediability score by examining the extent and timeliness of restoring the affected users to their former state prior to the materialisation of the inherent systemic risks. The scoring chart for the severity of inherent systemic risks, along with explanations for each scoring threshold, is available in Figure 6.

- **Integrated inherent systemic risk**: Finally, Whaleco multiplied the probability score by the severity risk scores to compute the integrated inherent systemic risk score. The integrated risk score was then translated into an integrated risk rating using a risk score matrix, as shown in Figure 7. The resulting inherent systemic risk score in turn dictated the level of management attention and required mitigation efforts.

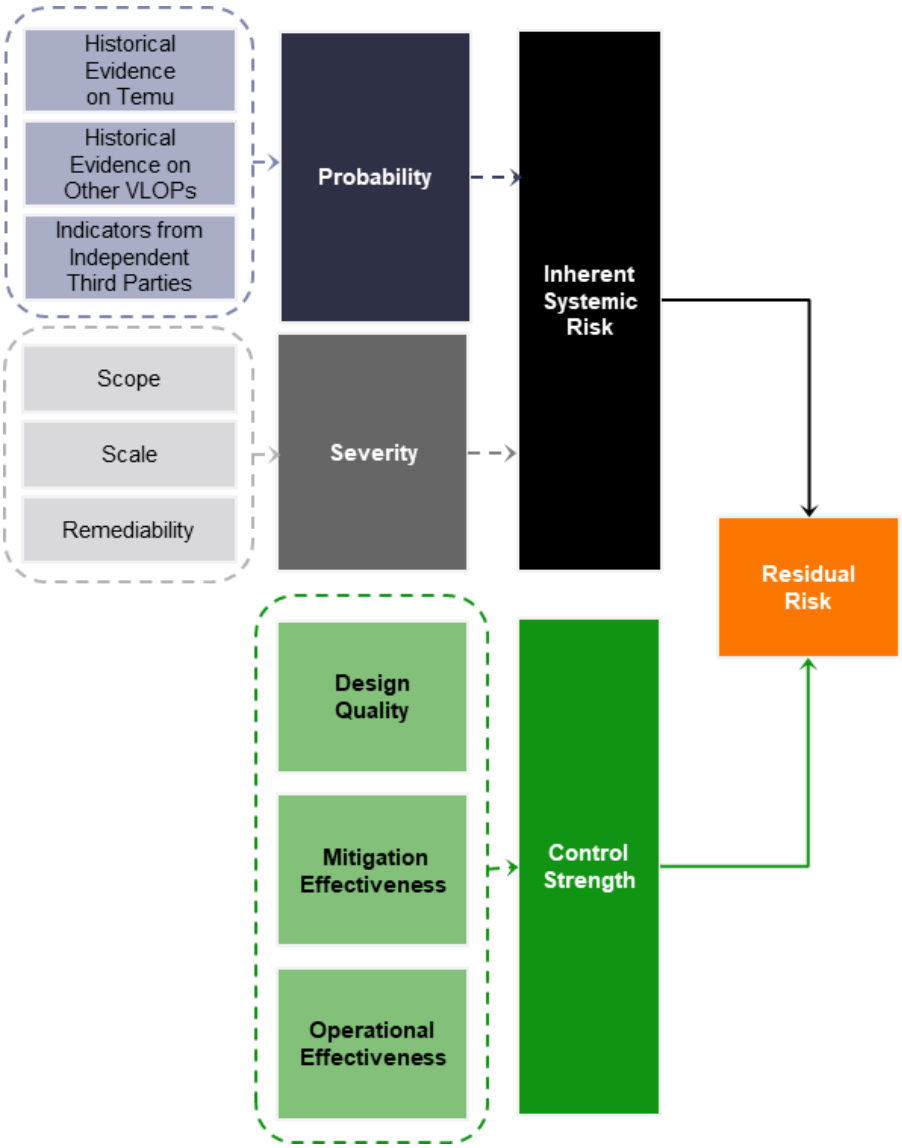


Figure 4: Whaleco's Risk Rating Methodology

Probability Conditions	Inherent Probability Matrix					
	N/A (0)	**Low (1)**	**Low-Medium (2)**	**Medium (3)**	**Medium-High (4)**	**High (5)**
Condition 1: Historical Occurrences of systemic risks on Temu	There is **no evidence of this risk ever having occurred on Temu or other marketplaces**, based on service features and functionalities, the use of the service, and the historical content and user behaviour on Temu and other online marketplaces, or as reported by regulators or reputable news sources.	There is no/very limited evidence of this risk occurring on Temu in the past 12 months, based the use of the service, and the historical content and user behaviour on Temu	There is evidence of this risk occurring on Temu multiple times over the past year, occasionally aligning with a quarterly pattern, but lacks monthly regularity, based the use of the service, and the historical content and user behaviour on Temu	There is evidence of this risk recurring on Temu with a frequency of one or more times per month, based on the use of the service, and the historical content and user behaviour on Temu	There is evidence of this risk occurring on Temu daily, based on the use of the service, and the historical content and user behaviour on Temu, but the prevalence rate is less than 1%* * Based on data from proactive control/prevention and penalties from user report (note: as an e-commerce platform, this calculation applies quantitatively to illegal content at the product-level only), regardless of whether the content was successfully published	There is evidence of this risk occurring on Temu daily, based on the use of the service, and the historical content and user behaviour on Temu, and the prevalence rate is greater than 1%* * Based on data from proactive control/prevention and penalties from user report (note: as an e-commerce platform, this calculation applies quantitatively to illegal content at the product-level only), regardless of whether the content was successfully published
Condition 2: Systemic risk occurrences on other VLOPs operating online marketplaces (via transparency reports)		There is no/very limited evidence of this risk occurring within other online marketplaces based on the last 2 published transparency reports	There is limited evidence of this risk, which appears on a minority of other online marketplaces and, where present, constitutes a low volume of enforcement actions based on the last 2 published transparency reports	There is evidence of this risk occurring more than half of other online marketplaces, where it is generally classified as a low-volume risk with a correspondingly low share of enforcement actions, based on the most recent published transparency reports	While there is consistent evidence of this risk occurring within all other online marketplaces, it is not considered a primary risk by volume, accounting for less than 10% of total penalties, based on the most recently published transparency report	There is consistent evidence of this risk occurring within all other online marketplaces based on the most recently published transparency report, where it also constitutes a primary risk by volume, making up more than 10% of total penalties
Condition 3: Systemic risk occurrences mentioned by regulators or market research		There are no/very limited reports of such risk on marketplaces based on market research, regulatory publications or media coverage	There is evidence of reports of such risk on marketplaces based on market research, regulatory publications or media coverage	There is repeated evidence of reports of such risk on marketplaces based on market research, regulatory publications or media coverage	There is consistent evidence of reports of such risk on marketplaces based on market research, regulatory publications or media coverage	Evidence consistently shows this is one of the most prevalent issues for marketplaces. This finding is substantiated by reports from top-tier sources, including national-level regulatory bodies, the European Commission, and leading international media

Figure 5: Whaleco's Risk Scoring Thresholds for Probability of Inherent Systemic Risks

Inherent Severity Matrix	**Severity score = (Scope + Scale + Remediability) / 3 Severity score ranges from 1 to 5**				
Severity Characteristics	**Low severity (1)**	**Low-Medium severity (2)**	**Medium severity (3)**	**Medium-High severity (4)**	**High severity (5)**
Scope: Number of individuals affected, on users and non-users, referring to both on-platform as well as societal harms	Localized to a limited user group or a rarely purchased product	Isolated disruption to a single country, a small feature, or a specific group of users	Impact across a regional user bases or a moderately used product	Significant impact across the entire EU user base, a critical product/frequently purchased product	Fundamental, platform-wide issue that affects core operations across EU markets
Scale: The extent to which the harm is physical, psychological, informational, economic, and/or societal; as well as how the harm may be experienced by vulnerable groups.	Impact would be unlikely to cause any physical, mental/emotional or financial harm, or any interference with fundamental rights	Impact could result in a minor physical, mental/emotional or financial harm, or a minor interference with fundamental rights	Impact is likely to result in moderate physical, mental/emotional or financial harm, or a moderate interference with fundamental rights OR Harm has the potential to impact vulnerable groups (e.g., minors and/or marginalised groups such as women, people with disabilities, elderly)	Impact is likely to result in significant physical, mental or emotional, or a significant interference with fundamental rights OR Harm particularly impacts vulnerable groups (e.g., minors and/or marginalised groups such as women, people with disabilities, elderly)	Impact is likely to result in death or irreversible physical or mental harm, or a severe impact to fundamental rights AND Harm particularly impacts vulnerable groups (e.g., minors and/or marginalised groups such as women, people with disabilities, elderly)
Remediability: Reversibility of the harm or difficulty in restoring the situation	Remedy will fully restore the person/situation to the state before the impact	Remedy will mostly restore the person/situation to the state before the impact	Remedy will partially restore the person/situation to the state before the impact	It is unlikely the remedy will restore the person/situation to the state before impact	The harm cannot be remedied through any means. No refund or product recall can be issued

Figure 6: Whaleco's Risk Scoring Chart for Severity of Inherent Systemic Risk

Inherent systemic risk matrix		Probability of Inherent Systemic Risk					
		N/A (0)	**Low (1)**	**Low-Medium (2)**	**Medium (3)**	**Medium-High (4)**	**High (5)**
Severity of Inherent Systemic Risk	Low (1)	N/A	Low (1)	Low (2)	Low (3)	Low-Medium (4)	Low-Medium (5)
	Low-Medium (2)	N/A	Low (2)	Low-Medium (4)	Low-Medium (6)	Low-Medium (8)	Medium (10)
	Medium (3)	N/A	Low (3)	Low-Medium (6)	Medium (9)	Medium (12)	Medium-High (15)
	Medium-High (4)	N/A	Low-Medium (4)	Low-Medium (8)	Medium (12)	Medium-High (16)	High (20)
	High (5)	N/A	Low-Medium (5)	Medium (10)	Medium-High (15)	High (20)	High (25)

Inherent systemic risk range	Inherent systemic risk level
$1 \leq x < 4$	Low
$4 \leq x < 9$	Low-Medium
$9 \leq x < 15$	Medium
$15 \leq x < 20$	Medium-High
$20 \leq x < 25$	High

Figure 7: Whaleco's Inherent Systemic Risk Matrix

Step 4: Assessing Control Strength

Following Whaleco's understanding of the inherent systemic risks associated with Temu, Whaleco analysed the control measures it put in place and assessed their effectiveness in mitigating these risks. To ensure an effective evaluation, Whaleco developed module-specific questions surrounding the six control groups within its DSA compliance framework, which it discussed in further detail in **Section VI: Temu's DSA Compliance Framework**:

- **Governance, risk & compliance (GRC) oversight**: controls related to board-level oversight, risk management policies, and regulatory compliance functions
- **Policies & standards**: development, maintenance, and enforcement of Whaleco's guidelines, terms of use, and other governance policies
- **User management & onboarding controls**: measures related to user age assurance, identity verification, trader blacklists, and trader education resources
- **Detection & enforcement**: a combination of automated and manual moderation systems used to detect and act on violative content and behaviour
- **User rights and remedies mechanisms**: systems for user appeals, notifications, and access to remedies, including out-of-court dispute settlement
- **External engagement**: engagement with law enforcement, trusted flaggers, and other external stakeholders to understand unknown risks

Whaleco evaluated the effectiveness of control measures across three dimensions: design quality, operational effectiveness, and mitigation effectiveness. This approach enabled the analysis of both the intentional design and the measured impact of the mitigation measures.

- **Design quality**: This dimension assesses how robust, targeted, and platform-specific the control is designed to be.
- **Operational effectiveness**: This dimension assesses whether the control is implemented consistently and is operating as intended.
- **Mitigation effectiveness and key risk indicators** (**"KRIs"**): This dimension measures the impact of the control in reducing the identified risk. Where possible, this evaluation is based on quantifiable evidence or through qualitative analyses of risk reduction.

Whaleco scored each question on a 1 (not effective) to 5 (highly effective) point scale, with each point corresponding to a defined level on Whaleco's control strength matrix. Whaleco then calculated a distinct percentage score for each of the three evaluation dimensions. Finally, Whaleco computed an integrated control strength score as the weighted average of the three-dimension scores, assigning 40% weight to "mitigation effectiveness and key risk indicators" and 30% each to "design quality" and "operational effectiveness". This weighting reflected a results-oriented approach, placing emphasis on the demonstrated, real-world impact of Temu's KRIs, while still valuing the design and operational factors that create effective risk controls.

Control Strength Matrix		5 Highly Effective	4 Mostly Effective	3 Somewhat Effective	2 Less Effective	1 Not Effective
Design quality:	Is it designed to mitigate the risk?	The control is robust and proven to target and mitigate against the risk on the platform, based on validation from an independent party (internal audit/SMEs) OR following documented testing and regular monitoring by internal Temu teams.	The control is proven to partially target and mitigate against the risk on the platform, based on validation by an independent party (internal audit/SMEs), with identified areas of improvement OR following monitoring by internal Temu teams.	The control is proven to somewhat mitigate against the risk on the platform, based on lack of validation by an independent party (internal audit/SMEs) OR following monitoring by internal Temu teams.	The control is limited in mitigating against the risk on the platform and it has not yet been validated by an independent party (internal audit/SMEs). There is no monitoring by internal Temu teams.	The control is proven to be ineffective in mitigating against the risk on the platform and it has not yet been validated by an independent party (internal audit/SMEs). There is no monitoring by internal Temu teams.
Operational Effectiveness:	Is it working as intended?	Controls are fully implemented, consistently applied, and working as intended. The processes are continuously improved. No deficiencies with control identified in the last 12 months.	Controls are implemented and working as intended, with minor improvements needed. No deficiencies with control identified in the last 12 months.	Controls are in place but inconsistently applied. No material deficiencies with control identified in the last 12 months.	Controls are poorly implemented. There has been a material deficiency identified with the control in the last 12 months.	There are no controls in place, planned actions have not been implemented, or control not working as intended.
Mitigation effectiveness and key risk indicators*:	How effectively is it mitigating the risk? *Key risk indicators will vary based on module. Below are suggested KRIs for the Illegal Content module, which will be used to assess the questions below tagged under Operational Effectiveness.	There is a clear reduction in residual risk on the service. Key Risk Indicators (KRIs) are consistently below the target threshold and show a clear, statistically significant reduction in residual risk. There is a strong, evidence-backed causal link between the control's operation and the positive outcome.	The controls somewhat reduce residual risk on the service. Key Risk Indicators (KRIs) are generally at or near target levels, with a clear downward trend in residual risk. The link between the control and the outcome is well-supported by data.	The control has a partial or mixed impact on risk reduction. While it contributes to risk reduction, the effect is not as significant as expected, or other factors are heavily influencing the outcome.	The control has a minimal or no discernible impact on risk reduction. Residual risk levels remain flat or are only slightly reduced. There is no clear evidence that the control is effective.	Key Risk Indicators show no reduction in residual risk, or the risk is actively worsening. The control has demonstrably failed to achieve its objective.

Figure 8: Whaleco's Control Strength Matrix

Step 5: Assessing Residual Risks

Residual risks are calculated using a matrix that incorporates both inherent systemic risk ratings and control strength ratings derived from the assessment steps outlined above. This matrix approach calculates residual risk levels by factoring the measured strength of existing controls against baseline inherent systemic risks.

Residual Risk Matrix			**Inherent Systemic Risk**				
			1	**2**	**3**	**4**	**5**
			Low	**Low-Medium**	**Medium**	**Medium-High**	**High**
Mitigation Effectiveness	Not Effective	< 60%	Low	Low-Medium	Medium	Medium-High	High
	Less Effective	>= 60%	Low	Low-Medium	Medium	Medium-High	High
	Somewhat Effective	>= 70%	Low	Low	Low-Medium	Medium	Medium-High
	Mostly Effective	>= 80%	Low	Low	Low	Low-Medium	Medium
	Highly Effective	>= 90%	Low	Low	Low	Low	Low-Medium

Figure 9: Residual Risk Matrix

In the area of most significant concern (i.e., illegal content), Whaleco leveraged a multi-layered validation framework to substantiate the reliability of its residual risk assessment results. More specifically, Whaleco strengthened the residual risk conclusions through evidence from the following sources:

- **External Intelligence and Regulatory Corroboration:** Continuous monitoring of public information and active engagement with EU authorities, consumer bodies, and industry associations, which provided qualitative validation of Temu's risk posture.

- **Internal Independent Verification:** A consumer-centric measurement programme conducted by an independent internal team, utilising Violative View Rate (VVR) and Violative Order Rate (VOR) metrics to quantitatively assess the actual or foreseeable negative effects on users.

- **Targeted Stress Testing and Collaborative Assessments:** Physical product testing ("mystery shopping") conducted with accredited laboratories and a Brand Cleanliness Testing Programme in direct collaboration with rights holders to probe for specific, non-obvious compliance issues.

This multi-faceted approach, combining broad quantitative measurement with qualitative external feedback and targeted deep dives, provides a robust and reliable validation of the residual risk assessment, complementing insights derived from internal operational data sources. Further details about these validation exercises are discussed in the module-specific assessments in **Section VI**.

Step 6: Identifying and Implementing Mitigation Enhancement Plans

The final step to Whaleco's methodology was identifying and implementing mitigation enhancement plans. This step follows the residual risk assessment and is designed to address areas where existing controls require bolstering. For each risk area, particularly those with a medium or higher residual risk, Whaleco would evaluate and identify specific measures to be strengthened or newly implemented. The purpose of these plans is to systematically reduce residual risk and enhance Temu's overall safety year on year. This process ensures a commitment to continuous improvement, acknowledging that risks on online marketplaces are dynamic and require ongoing attention.

IV. Overview of Key Temu Attributes

As discussed in Section III above, an essential step in Whaleco's risk assessment methodology was mapping the core characteristics, other features and services, and DSA Article 34(2) influencing factors that can give rise to systemic risks or be used, exploited, or manipulated by traders, users, or other third parties to elevate or disseminate the risks. Whaleco discusses below the key attributes Temu offers and how they work.

A. Core Characteristics

Trader network: Through Temu, Whaleco hosts an extensive community of traders who list, promote, and sell products to EU users. During the Relevant Period, Temu hosts more than [Confidential] traders, both from within and outside the EU, who have listed products for sale to EU users. Temu offers market access to enterprises of all sizes, including small and medium-sized businesses that may lack direct access to the EU market. All traders operate as independent third parties with no affiliation to Whaleco. Whaleco neither manufactures nor oversees the manufacturing of products sold on Temu.

Product portfolio: Temu provides intermediary infrastructure for traders to list a large number of product listings that are subject to varied product compliance regulations in the EU. Temu does not own, sell, or hold title to any products listed on Temu.

User base: Temu currently has a broad EU user base with approximately 108 million monthly active EU users during the Relevant Period. According to its Terms of Use, access to Temu is intended for adult users only.

Distance-sales model: Sales on Temu are of a distant nature, which means EU consumers make purchasing decisions on the basis of product information provided on Temu and complete transactions remotely with traders.

B. Other Services and Features

Product reviews: Temu offers a product review function to assist consumers in making informed purchasing decisions. Temu displays product reviews through two entrances: (1) a trader's store homepage which aggregates reviews related to all products offered by that trader and (2) a specific product listing's dedicated review section. Product reviews may include text, images, and videos.

Only consumers who purchased relevant products can submit reviews for products they have bought. Other users can access reviewers' public profiles, share reviews on third-party platforms, and mark reviews as "helpful" or report policy violations, but they cannot reply to or comment on product reviews.

Limited chat function: Temu provides chat functionality only for authentic purchase-related exchanges between traders and consumers. No chat function is available on individual product listing pages or store homepages. After consumers place orders, messaging becomes accessible through order details, logistics tracking, and after-sales service pages for traders and consumers to chat. The chats are also subject to content moderation. Traders cannot message other traders, and consumers cannot message other consumers.

Report and appealing systems: Temu provides reporting and appealing mechanisms for all users. Users can use the "Report this item" feature for prohibited, unsafe, or non-compliant products, the "Report this review" function for problematic reviews, and a dedicated IP channel, the IP Portal, for

alleged IP infringements. Valid claims lead to immediate content removal, with email notifications to the reporters.

Traders whose onboarding applications are rejected, users subject to a Temu-restrictive measure, or users dissatisfied with the outcome of a report are provided with appeal channels to lodge complaints for a period of at least six months following the decision being appealed. All appeals undergo human review. Whaleco reverses the initial decision if an appeal is upheld. If a user remains dissatisfied with the final decision, Whaleco provides clear guidance for affected users to seek further redress through out-of-court dispute settlement mechanisms pursuant to Article 21 of the DSA.

Customer services: Whaleco's customer service primarily addresses 1) transactional issues, including logistics inquiries, order cancellations, returns, and refunds, and 2) questions about Temu services and features, such as language settings and details of promotional activities. Consumers may cancel orders at any time before shipment. Whaleco fulfils its obligations regarding the statutory right of withdrawal under the Consumer Rights Directive and, without prejudice to those rights, voluntarily offers a 90-day return policy for most purchases with free shipping for the first return for each order. The Temu Purchase Protection Program provides additional assurance by guaranteeing a full refund where items are mismatched, damaged, undelivered, delivered late, or lost. Customers can access these services via the customer support chatbot, live chat, or call-back hotlines.

Whaleco's customer-service representatives act as an intermediary when consumers encounter difficulties exercising their rights vis-à-vis traders. Under the Temu Seller EU Services Agreement, traders must provide after-sales support, including cancellations, returns, exchanges, and refunds. At a customer's request, Whaleco mediates communications and facilitates the resolution of disputes between the customer and the trader.

Logistics: Whaleco partners with third-party logistics service providers from whom traders may select for order fulfilment. Consumers receive transparent shipping options and delivery estimates at checkout, with Whaleco providing dispute mediation for logistics-related issues such as delivery delays or failures.

Payment: Temu has a standardised checkout process that provides clear, upfront disclosure of the full cost before purchase. Whaleco engages third-party payment service providers to deliver payment services, including but not limited to collection, processing, refund, settlement, and payout. Consumers must make payments using an electronic payment method (e.g., credit card).

On-platform promotional activities: Temu offers promotional benefits, including discounts, coupons, and purchase credits, through on-platform promotional activities such as seasonal campaigns, thematic promotions, or personalised offers. Consumers can explore various ways to participate in the activities and maintain discretion to accept, decline, or exit promotional activities according to their preferences.

Off-platform promotional activities: Temu facilitates promotional activities on third-party platforms to market products and events, such as contracting with qualified influencers who develop promotional content and the A&I Programme, which allows eligible users to sign up as Affiliates or Influencers to share direct links and promotional codes in exchange for commissions.

C. DSA 34(2) Influencing Factors

Recommender systems and related algorithmic systems: Temu utilises recommender systems to organise and present its extensive product catalogue, on-platform promotional content, and product

reviews to EU consumers. The goal is to make the shopping experience intuitive and efficient by helping consumers discover relevant content.

Temu's product catalogue and on-platform promotional activities are displayed using a combination of factors related to user interactions with Temu (views, clicks, add-to-carts, purchases, etc.), product features (title, price, category, sales volume, etc.), and contextual features (device information, region, language setting, etc.). The systems do not identify or infer sensitive user characteristics such as gender, race, ethnicity, political opinions or religious beliefs. Product reviews are displayed without personalisation and ranked only by regional relevance and review quality. The effectiveness of these systems is measured by their ability to surface content that aligns with consumers' interests. Where available, consumers can adjust what they see using filtering and sorting controls, and they have the option to turn off personalised recommendations.

To maintain platform integrity and user safety, Temu's recommender system includes built-in mechanisms to automatically exclude or reduce visibility of products unsuitable for proactive recommendations. Query safeguards prevent auto-complete suggestions and withhold search results when users submit queries containing non-compliant terms. For instance, if a user types partially non-compliant keywords (e.g., "child la"), the system will not display the complete prohibited term in suggestions (here, "child labour/labor"), and if a prohibited term is entered (here, "child labour/labor"), no search suggestions or product listings will appear. These safeguards are available across all official EU languages through real-time translation functionality.

Content moderation systems: Whaleco provides Temu-wide content moderation utilising automated detection and human review, with continuous pre- and post-publication monitoring. Automated detection applies keyword and image recognition; the content moderation workforce is regularly trained and includes a dedicated team for notice and action mechanisms pursuant to Article 16 DSA.

Whaleco maintains strict policies prohibiting illegal content. When violations are detected, Whaleco takes prompt action ranging from content or listing removal to account suspension. This proactive approach, together with reactive measures for handling reports as well as regulatory notices, underpins Whaleco's content moderation efforts and helps maintain standards across Temu.

Terms and conditions and their enforcement: Whaleco maintains a comprehensive legal framework governing the relationship with Temu users. It is principally anchored in Temu's Terms of Use and Temu Seller EU Services Agreement, together with policies referenced therein. The principal documents include, among others:

- **Terms of Use**: These terms establish a binding contract with users, including (among other matters) user requirements and registration, rules and restrictions, purchase and payment, limitation of liability, and references to other applicable policies.

- **Temu Seller EU Services Agreement**: This agreement sets contractual terms for EU traders, including (among other matters) service content and fees, trader eligibility and onboarding process, product listing standards, compliance with applicable laws and rules, performance obligations, and complaints and mediation mechanisms.

- **Temu Product Safety and Compliance Policy**: This policy sets trader obligations to ensure listed products are safe and compliant with applicable laws, industry and safety standards, and Temu policies, including (among other matters) prohibited/restricted product categories, compliance requirements for specific product categories, mandatory safety standards and certification requirements, as well as labelling and documentation obligations.

- **Community Guidelines**: These guidelines establish standards for appropriate user conduct and content across Temu features such as reviews, profiles, and user interactions, including (among other matters) prohibitions on unethical conduct, distracting content and spam, sharing of private information, objectionable content, hate speech and discrimination, sexual content, and external links, to ensure a safe and beneficial experience for all users.

These documents define the rights and responsibilities of all parties, establish rules for acceptable content and conduct, specify prohibited activities, and provide the legal basis for enforcement actions. Acceptance of these terms and conditions is mandatory for accessing Temu's EU-facing services. Violations may lead to content or listing removal, and in serious cases, account suspension. These legal documents are regularly reviewed and updated to reflect changes in law, policy, and Temu operations.

On-platform advertising system: During the Relevant Period, Temu did not operate an on-platform advertising system permitting eligible traders to pay to promote their product listings into more prominent positions.

Data-related practices: Whaleco collects data necessary for marketplace operations. EU user data is stored by default within European cloud infrastructure and protected through technical and organisational measures preventing unauthorised access, loss, theft, or misuse.

Temu's Privacy Policy provides clear, accessible information on data processing practices and enables users to exercise control over their personal data through implemented mechanisms. The policy undergoes regular updates to maintain compliance with the General Data Protection Regulation ("GDPR"), the Privacy and Electronic Communications Directive 2002/58/EC (ePrivacy Directive), the Charter of Fundamental Rights of the EU, the European Convention on Human Rights, and European Court of Human Rights decisions.

V. Temu's Risk Governance Framework

Whaleco fosters a safe and trustworthy marketplace through a comprehensive, multi-layered system of controls that guide and protect users and traders at every stage of their platform journey. These controls are applied across the product lifecycle, from proactively identifying and preventing risks before they arise, to enabling swift response and remediation should they materialise. Each incident further strengthens Whaleco's evolving moderation framework, turning experience into enhanced safeguards. This dynamic and iterative process allows Whaleco to manage platform risks with efficiency, resilience, and consistency, while continuously adapting to new regulatory standards, technological change, and evolving user behaviour.

In line with Article 35(1) of the DSA and industry best practices, Whaleco has designed six distinct yet deeply interconnected control domains and employs evidence-based and data-driven assessments to evaluate the design quality, operational and mitigation effectiveness of these controls.

As illustrated above, Whaleco maintains controls organised into six control domains. Whaleco's mitigation framework combines measures that are applied platform-wide with those tailored to specific modules. This subsection focuses on the foundational controls applied across all modules, which form the backbone of Temu's Risk Governance Framework. For details on module-specific controls, please refer to the corresponding modules.

A. Governance, Risk & Compliance Oversight (GRC)

In line with Article 34 DSA, Whaleco's Board of Directors is responsible for approving and reviewing strategies and policies for identifying, managing, monitoring and mitigating systemic risks.

In addition to the Board, Whaleco has established a [Board-approved delegated decision-making] structure for certain DSA matters, along with a governance structure for the DSA Complianc7e Function, which outlines roles, responsibilities, reporting lines, and the independence of that function. The DSA Compliance Function is independent of Whaleco's day-to-day operations and is led by the Head of the DSA Compliance Function ("**HOCF"**), who is directly appointed by the Board.

The DSA Compliance Function works closely with internal stakeholders, including the LCT and TST, to oversee the compliance and efficacy of the risk assessment process, ensure that all risks referred to in Article 34 of the DSA are identified and properly reported on, and that reasonable, proportionate, and effective mitigation measures are taken pursuant to Article 35 of the DSA. Adequate resources are allocated to the LCT, TST, the DSA Compliance Function, and the technical team, with dedicated teams covering legal, product safety, content moderation, and data security. This structure ensures that the HOCF has the authority and independence necessary to challenge business decisions and to escalate systemic risks directly to the Board where required.

B. Policies & Standards

Whaleco's risk governance framework is underpinned by a set of platform-wide policies and standards, including the Terms of Use, Seller EU Services Agreement, Product Safety and Compliance Policy, Privacy Policy, Intellectual Property Policy, and Community Guidelines. These documents define the rights and responsibilities of both consumers and traders, set clear boundaries for what may be provided or shared on Temu, and establish the standards against which enforcement actions are conducted.

The development and implementation of these policies are carried out collaboratively by the TST and LCT. To ensure that the rules remain current and effective, Temu consults external legal counsel, industry experts, and relevant organisations. Feedback from these stakeholders, combined with consideration of the internal governance practice, informs the continuous refinement of its standards.

In addition, Whaleco continuously monitors regulatory updates and feedback from regulators to ensure compliance with the latest laws and legislation. Whaleco also maintains a user-friendly, easily accessible Transparency Center, which hosts the key policies referenced above to help users and regulators understand the rules and how they are applied in practice.

C. User Management & Onboarding Control

This process serves as Whaleco's first line of defence. During onboarding, Whaleco collects, stores and processes user information in compliance with its Privacy Policy and other applicable laws and policies. For traders, the required information extends beyond basic contact details and includes business registration documents, legal representative identification, and other critical information necessary for traceability. This process is followed by a rigorous verification procedure. Automated screening first analyses submitted information for irregularities and obvious errors. If inconsistency is identified, the application is further progressed to manual review for evaluation. This verification procedure includes cross-referencing the provided information with third-party databases to verify their reliability and completeness. Furthermore, Whaleco screens all prospective traders against its internal "Trader Blocklist", which aggregates sanction lists from global regulatory authorities to prevent high-risk sanctioned entities from gaining access to Temu. Whaleco also maintains a separate

onboarding restriction list to block identified rogue traders found to have engaged in deliberate or repeated misconduct from re-entering Temu, even with a new identity. This scrutiny continues after the trader's successful registration to ensure ongoing integrity of its trader community.

Following onboarding, Whaleco provides a suite of policies and rules designed to help users and traders fully understand their rights and responsibilities when using Temu's services. A key component is its comprehensive trader education programme, which is specifically developed to equip traders with the knowledge and tools necessary to successfully set up their shops, deliver compliant products and maintain awareness of their obligations under applicable laws.

D. Detection & Enforcement

At the heart of Whaleco's mitigation framework is a moderation system that combines automated detection with human reviews. This integrated approach is designed to proactively detect, intercept and remove non-compliant product listings and content that violate Temu's rules and policies. The system also collects and analyses user behaviour to flag potential bad-faith actors.

The automated screening utilises sophisticated text and image recognition tools to analyse consumer- and trader-generated content, identifying potentially non-compliant product listings or content both before and after publication on Temu. Potentially violative product listings or content detected are promptly removed, and a clear statement of reasons ("**SOR**") is provided to the affected user or trader, explaining the decision and outlining their right to appeal. Cases where automated detection is inconclusive are escalated to human moderators for final adjudication.

Complementing this proactive moderation, Whaleco has also developed reactive moderation capabilities by establishing processes for receiving and acting on external reports. A key feature is the dedicated reporting function, which allows users, rights holders, and other relevant stakeholders to flag potentially non-compliant products or reviews. All submitted reports are assigned to human moderators for review. If a report is validated, remedial actions are promptly initiated, including the swift removal of the potentially non-compliant content from Temu.

To ensure accountability, Whaleco also deploys a structured penalty scheme for traders. For repeated offenders and severe violations, this includes stringent measures such as service suspension and permanent blocklisting, effectively barring bad-faith actors from Temu.

Human review forms a substantial part of Whaleco's content moderation system and provides an important safeguard within the process. All moderators complete structured onboarding training, meet accuracy and throughput standards, and receive ongoing coaching in specialised areas such as IP, sensitive product content, and emerging risks, thereby driving continuous improvement and adaptability to new regulatory requirements and market dynamics. Knowledge sharing is embedded through team discussions, and multilingual moderators enable consistent enforcement across the EU.

E. User Rights and Redress Mechanisms

Whaleco recognises that equal and transparent participation in the marketplace is a fundamental right for all users of Temu. Both consumers and traders are entitled to fair access to marketplace services without discrimination, provided they comply with the Terms of Use, Seller EU Services Agreement, and other applicable rules. To safeguard this principle, Whaleco ensures that platform decisions—such as the removal of a product listing, the restriction of account privileges, or the dismissal of a report—are accompanied by a clear SOR or notification and supported by effective redress mechanisms. Where a consumer or trader disagrees with a decision, they may submit an appeal directly through the link provided in the SOR or the notification. Appeals are reviewed by dedicated staff. If an appeal is

successful, Whaleco promptly restores the affected product, account access, or service status. In addition, Whaleco provides both consumers and traders with sufficient information about the possibility of seeking remedies through out-of-court dispute settlement bodies.

F. External Engagement

Whaleco highly values feedback from external stakeholders and actively uses these insights to enhance its practices. By maintaining open and constructive dialogue, Whaleco continuously reviews and incorporates recommendations, as well as industry best practices, into its compliance framework to ensure ongoing improvement and responsiveness. During the Relevant Period, Whaleco actively participated in high-profile industry seminars and maintained active engagement with regulatory bodies and industry associations.

VI. Product Compliance, IP, and Content Compliance

As an online marketplace hosting an enormous, diverse, and global third-party trader base, Temu faces inherent systemic risks of misuse by traders attempting to distribute inauthentic or unsafe (i.e., illegal) products and users that may distribute illegal content through reviews and chats. This module identifies and assesses the systemic risks of dissemination of illegal content on Temu pursuant to Article 34(1)(a) and Recital 80 of the DSA. The assessment is structured into three sub-modules:

- The **Product Compliance** risk sub-module assesses the risk that traders may use Temu to list, promote, or sell products that are prohibited, restricted or otherwise non-compliant under applicable EU or Member State law, as well as Temu's terms and conditions.

- The **IP** risk sub-module assesses the risk that traders may use Temu to disseminate products that infringe third parties' IP rights, including trademarks, copyrights, patents, and design rights defined under applicable laws of the EU and the EU Member States.

- The **Content Compliance** risk sub-module assesses the risk of misuse of Temu's limited user-generated content ("**UGC**") functionalities to disseminate other forms of non-compliant content, such as discriminatory or hate speech, violent content, unauthorised sharing of private images, and other content violating Temu's Community Guidelines and relevant platform policies.

The systemic risks associated with dissemination of illegal content have significant cross-module implications. For example, prohibited products could impair the rights of consumers and minors as enshrined in the Charter of Fundamental Rights of the EU. Consequently, the mitigation measures detailed within this module—especially those related to trader verification, content moderation, and user redress mechanisms—form the cornerstone of Temu's broader risk mitigation framework and are broadly relevant to the other modules. For efficiency, this module discusses these foundational mitigation measures in depth, whereas the subsequent modules will reference these controls to the extent they are relevant and will instead focus on discussing unique mitigation measures tailored to the specific risks under the subsequent modules.

A. 2025 Highlights

In Year 2, the EU regulatory framework for online platforms transitioned from legislation to enforcement, creating a landscape of intertwined legal obligations. For example, Article 30 of the DSA and the GPSR impose layered obligations on Temu in relation to compliance management of traders selling to EU consumers. The intricacies of the regulatory landscape necessitated holistic compliance strategies beyond the management of discrete regulatory tasks. The cumulative effect of these compliance mandates ensures that only mature, reliable, and compliant traders will ultimately meet the necessary standards to continue offering reliable products to EU consumers. In addition, major events created moments of heightened risk. The 2024 Paris Olympics, for example, created heightened risks of counterfeit Olympic-themed products on Temu, prompting Whaleco to implement enhanced monitoring and enforcement measures.

In response to these emerging challenges, Whaleco continued to invest in technology capabilities and human resources in trader compliance and content moderation. The Seller Education Programme, a cornerstone of Whaleco's preventative strategy to enhance trader compliance awareness, generated over 8 million views during the Relevant Period. Continuous awareness training led to improvements in trader compliance, [Confidential] Regarding proactive moderation, Whaleco upgraded product safety and information verification systems to align with DSA and GPSR requirements. [Confidential] Whaleco proactively engaged with external stakeholders during the Relevant Period, such as with the EU-funded

SPEAC Safe Non-Food Consumer Products in the EU and China ("**SPEAC**") project to enhance trader compliance and product safety awareness. These concerted efforts led to more than 99% of enforcement actions against illegal content being taken proactively through Whaleco's own initiatives prior to external notifications. Cases flagged by external sources were promptly handled by a well-resourced team within a median response time of 24 hours. [Confidential]

Nevertheless, Whaleco recognises that mitigating systemic risk requires relentless effort and substantial work remains. Whaleco is committed to continuous improve5,000 brandsment, enhanced transparency, and proactive engagement with stakeholders to further mitigate systemic risks. Whaleco recently launched a Transparency Center which, together with the DSA Page and the DSA Help Page, serve as a resource hub for compliance policies, DSA-related functionalities, and enforcement activities. Whaleco will continue to leverage the Transparency Center to host enhanced disclosures and compliance updates. Whaleco will expand its engagement with external organisations and industry associations to gather feedback and share insights. Last, Whaleco plans to collaborate with external expert organisations to develop advanced sets of metrics for assessments of systemic risks.

Below is a snapshot of Whaleco's risk assessment results.

Sub-Module	Inherent Systemic Risk	Control Strength	Residual Risk
Product Compliance	High (5/5)	Mostly Effective (4/5)	Medium (3/5)
IP	Medium-High (4/5)	Mostly Effective (4/5)	Low-Medium (2/5)
Content Compliance	Medium (3/5)	Mostly Effective (4/5)	Low (1/5)
Overall	High (5/5)	Mostly Effective (4/5)	Medium (3/5)

B. Assessment of the Systemic Risks

Pursuant to Article 34(1)(a) of the DSA, Whaleco identifies, analyses, and assesses whether and how the systemic risks of dissemination of illegal content could potentially materialise through Temu's design, functionalities, or the use made of Temu's services by traders, users, or other third parties. In accordance with Recital 80 of the DSA, this assessment is further divided into three sub-modules: Product Compliance, IP, and Content Compliance. For efficiency, where a Temu attribute or the use made of it is assessed to have a similar influence on more than one of the sub-modules, Whaleco integrates the related discussions. Further, while Whaleco conducted risk assessments for all the Temu attributes and influencing factors mapped in **Section IV: Overview of Key Temu Attributes**, the following discussion focuses on the factors that are assessed to have a substantial impact on the risks of dissemination of illegal content.

The following paragraphs examine, in the hypothetical scenario where no mitigation controls were in place, whether and how Temu's core characteristics, other services and features, as well as the influencing factors specified in Article 34(2) of the DSA could give rise to the inherent systemic risks of dissemination of illegal content.

i. Core Characteristics

Each of Temu's four core characteristics, i.e., (1) hosting traders, (2) hosting product listings, (3) accommodating EU users, and (4) facilitating online marketplace sales, influences and in some cases

defines Temu's inherent systemic risk landscape in relation to the dissemination of prohibited, restricted, IP-infringing products, and violative content.

As an online marketplace, Temu hosts a large and diverse trader base comprising both EU and non-EU traders who list, promote, and sell products to EU consumers. Without effective governance and control mechanisms, certain traders may intentionally exploit or negligently misuse Temu services to list non-compliant products, including those infringing IP rights and prohibited and restricted products. Whaleco identified and assessed that the following factors in relation to Temu's core characteristics might give rise to or otherwise influence the probability or severity of illegal content risks:

- **Lack of compliance awareness among non-EU traders**: While Temu's cross-border and diverse trader community enhances product variety, it also contributes to the likelihood that certain third-party traders, in particular those based outside of the EU, may lack sufficient knowledge of applicable EU legislation governing product safety, IP protection, and digital commerce or the recent legislative updates or amendments. Additionally, the technical nature of certain regulatory requirements may present comprehension barriers for traders. Without sufficient awareness training, certain traders may inadvertently list non-compliant products on EU country sites.

- **Non-compliant qualification, authorisations, and information:** For branded products and products requiring specific qualifications for sale, Temu requires traders to provide authorisation letters, legitimate proof of source, and relevant certifications, such as test reports or Conformité Européenne ("**CE"**) marking. However, traders may attempt to circumvent Temu's controls by submitting non-compliant qualification documents or authorisation letters. Additionally, traders may attempt to submit non-compliant product information, manipulated images, or disguise keywords to evade Whaleco's existing safeguards.

- **Product misclassification:** Certain traders may intentionally or inadvertently miscategorise their products into less scrutinised product categories to circumvent category-specific controls and safety requirements. Without tailored mitigation measures, such exploitation attempts could undermine the integrity of categorisation systems designed to ensure products receive risk-appropriate levels of scrutiny.

- **Repeat violations and reappearance of non-compliant products:** Traders may repeatedly list non-compliant products. [Confidential] Further, traders may misuse Temu's services or design to relist previously removed non-compliant products by making superficial alterations to product attributes, such as titles, descriptions, or product images. Traders who are suspended due to repeated listings of non-compliant content may attempt to reappear on Temu using the same or different identities. Without adequate controls, this pattern of behaviour could lead to the recurrence of dissemination of non-compliant content.

- **Scale of product listings and EU user base:** The large volume of product listings, combined with the continuous influx of new products from traders with varying levels of sophistication, contributes to the likelihood that prohibited, restricted, or IP-infringing products may be introduced to the marketplace. The diverse nature of product listings also creates challenges for Temu to detect and remove non-compliant products, as different product categories may be subject to divergent product compliance or IP protection requirements. [Confidential] This distribution suggests that users are more likely to be exposed to everyday-use items from lower-risk product categories. However, Temu's large EU active user base means that a considerable EU population could be exposed to illegal products through their viewing and purchasing of these products on Temu.

- **Lack of brick-and-mortar guardrails:** The distant nature of sales on Temu suggests that consumers lack certain checkpoints available in traditional brick-and-mortar shopping experiences, such as physically examining product quality or identifying potential counterfeits. In addition, in the absence of Temu's user redress mechanisms, consumers may face difficulties in remedying damages resulting from the sale of illegal products by traders without a local presence.

ii. Services and features

Specific Temu functionalities, as outlined below, while designed to enhance the user experience, may also influence the potential dissemination of illegal content. A detailed description of these features is available in **Section IV** of this Report.

- **Review system:** Temu's review system enables consumers who have purchased relevant products to post publicly available reviews of their shopping experiences. The ability for users to post text, images, and videos in reviews could be misused to disseminate illegal content, including false information that harms traders' reputations or artificially inflates product ratings, reviews, or sales volume in collusion with traders. In addition, users may post inappropriate content (such as hate speech, sexually explicit material, or any other content that violates Temu's Community Guidelines) or embed in their reviews' external links or visual media that contain inconspicuous violations. During the Relevant Period, Whaleco identified and removed over 89,000 non-compliant contents from the review function through its own-initiated monitoring and external feedback.

- **Limited chat function:** The chat function for trader–consumer interactions is designed to provide EU consumers with a convenient channel to contact traders. However, both traders and consumers may misuse this function to share content that violates Temu's Community Guidelines, thereby undermining the experience of the other party. In addition, traders may misuse this function to divert consumers to third-party platforms for purchases, circumventing Temu's governance measures. To mitigate this, Whaleco has built in counteracting safeguards into its infrastructure, including a controlled communication feature that allows interaction strictly between buyers and traders only after a valid order has been placed. These designs effectively minimise the inherent systemic risks of potential manipulation, and therefore, Whaleco assesses that the additional risk of dissemination of illegal content that this feature may create is modest.

- **Report and appealing systems:** The design and accessibility of reporting and appeal mechanisms are critical, as ineffective systems could fail to capture essential user feedback, hindering Temu's ability to detect and remove non-compliant products or other content. Effective reporting and appeal mechanisms could instead provide sufficient deterrence against attempts by traders to list illegal products or content.

- **Customer services:** The customer service channel serves as an important mechanism that enables users to promptly seek redress if they purchased non-compliant or infringing products. Lack of easy access to the channel may prevent users from obtaining timely and effective remedies.

- **On-platform promotional activities:** When non-compliant products bypass Whaleco's proactive detection measures, they could be included in Temu's on-platform promotional activities, which could amplify their dissemination on Temu and reach more EU users. Internal data for the Relevant Period indicated that the vast majority of products exposed to users through on-platform promotional activities were compliant. Only a small share exposed via this

channel was later identified through external feedback[1] as potentially non-compliant products. [Confidential]

- **Off-platform promotional activities:** The A&I Programme extends the reach of product listings on Temu to users of third-party platforms, who may otherwise lack visibility of the product listings. This creates a risk that, without sufficient controls, non-compliant products could be enrolled in the A&I Programme and receive promotion off-platform, which could expose a broader EU population to the non-compliant products. Further, Affiliates and Influencers could generate untruthful or non-compliant information to mislead the audience into making incorrect purchasing decisions. Internal data for the Relevant Period indicated that the vast majority of products exposed to users through the A&I Programme were compliant. [Confidential]

iii. DSA 34(2) influencing factors

Whaleco has further evaluated the specific influencing factors outlined in Article 34(2) of the DSA, and their potential impact on the systemic risk related to dissemination of illegal content on Temu. Detailed descriptions of these influencing factors are available in **Section IV** of this Report.

- **Recommender systems:** In the absence of effective controls, recommender systems and relevant algorithmic systems could amplify the reach of illegal content that has bypassed proactive detection by promoting it to more prominent locations on Temu. Internal data for the Relevant Period indicated that the vast majority of products exposed to users through Temu's recommender systems were compliant. [Confidential]

- **Content moderation systems:** Whaleco has implemented content moderation systems to mitigate risks related to product compliance, IP, and content compliance. These systems serve as the cornerstone of Whaleco's mitigation controls, combining automated detection with human oversight to address the risk of illegal content. However, if the content moderation system cannot effectively enforce the platform's terms and conditions (such as reduced efficiency due to untrained recognition tools or a shortage of adequately trained reviewers), relevant risks may go undetected or missed, potentially resulting in systemic risks. During the Relevant Period, Temu's moderation systems removed over 103 million product listings for potential Product Compliance violations and over 38 million for potential IP Infringements within the EU. The vast majority of these actions were initiated proactively, with a proactive action rate of 99.99% for Product Compliance and 99.71% for IP. Additionally, over 89,000 pieces of non-compliant contents from the review function were intercepted and removed for Content Compliance violations with the EU, with a proactive rate of 99.64%.

- **Applicable terms and conditions and their enforcement:** Given the existence of both EU and numerous Member State laws and regulations, which are continuously evolving, Temu Terms of Use and Seller EU Services Agreement may, if not promptly updated, fail to address certain risks that require mitigation. This may contribute to or create risks of traders intentionally and inadvertently listing non-compliant content.

- **Systems for selecting and presenting advertisements:** During the Relevant Period, Temu did not have an on-platform advertising system.

[1] External feedback refers to different sources depending on the subject matter: for product compliance, feedback primarily comes from users and regulators; for IP, feedback primarily comes from rights holders.

- **Data-related practices:** Whaleco's data practices are essential factors for reducing systemic risks of illegal content dissemination. Data-related practices enable Temu to collect and use trader and user data to detect, investigate, and address infringements. Without such data-related practices, Temu would face significant challenges in accessing the trader and user data necessary to detect, investigate, or remediate instances of illegal content dissemination.

iv. Inherent systemic risk evaluation

The inherent systemic risk assessment evaluates the probability and severity of systemic risks in the hypothetical absence of any mitigation measures. Details of Whaleco's methodology for inherent systemic risk assessments are available in **Section III**. The overall inherent systemic risk for the Illegal Content module is assessed as "**High**".

A summary of the evaluation for each sub-module is provided below, outlining the factors considered for both probability and severity, respectively.

Sub-module	Inherent Systemic Risk Score	Assessment Findings
Product Compliance	**High**	**Probability (High - 5/5):** For Product Compliance, high enforcement volumes on Temu and other VLOPs operating online marketplaces and numerous regulatory reports on unsafe products online confirms a high likelihood of occurrence.
		Severity (High - 5/5): For Product Compliance, the inherent potential harm is assessed as severe, with a platform-wide scope, a scale that includes irreversible physical injury or death, and limited remediability through financial compensation alone.
IP	**Medium-High**	**Probability (High - 5/5):** For IP, evidence from all three dimensions, including high volumes of enforcement on Temu and other VLOPs operating online marketplaces, and numerous regulatory reports on IP infringements, confirms a high probability of occurrence.
		Severity (Medium - 3/5): For IP, the scope of harm is significant considering the large number of EU users that could potentially be affected. However, the primary harm is economic in nature, impacting both consumers and rights holders, and is considered less severe than physical or psychological harm. Consumers' economic harm can be remediated to some extent through refunds, and rights holders may seek reliefs by enforcing their IP rights. Considering these factors, the overall severity is thus assessed as medium.
Content Compliance	**Medium**	**Probability (Medium - 3/5):** As an e-commerce platform where publicly available user-generated content is primarily limited to product reviews, the likelihood of systemic dissemination of other forms of illegal content (e.g., hate speech) is moderate when compared to social media platforms, a conclusion supported by the lower volume of related enforcement actions in peer marketplace transparency reports.
		Severity (Medium - 3/5): Based on a review of past incidents, the scope is more limited compared to product-related risks. While the potential scale of harm could be severe and long-lasting, particularly

		for vulnerable groups, historical cases of moderated content on the platform have generally been confined to product-related complaints which can be effectively remedied through timely content removal and user support.

C. Mitigation Measures

Following Whaleco's identification, analyses, and assessment of how Temu's characteristics, services, and features influence its inherent systemic risks of dissemination of illegal content, Whaleco has developed a framework of mitigation measures. Some of these measures address risks common to all three sub-modules, with certain safeguards tailored specifically to individual sub-modules.

Whaleco broadly organises the measures into two categories: (i) measures aligned with the six defined control groups and (ii) those addressing platform-specific attributes such as recommender systems and the A&I Programme that could influence dissemination of illegal content on Temu. Together, these measures systematically mitigate systemic risks related to Product Compliance, IP, and Content Compliance, with effectiveness assessed through defined performance metrics and fact-finding questions developed in accordance with the methodology outlined in **Section III**. Based on Whaleco's evaluation, the overall effectiveness of controls with respect to the Illegal Content module is assessed as "**Mostly Effective**".

i. Governance, Risk & Compliance Oversight (GRC)

Whaleco's GRC framework for illegal content modules is managed by the TST, which addresses systemic risks by setting and enforcing standards across Product Compliance, IP, and Content Compliance domains. The framework integrates automated detection with rapid response protocols to process signals from internal systems as well as reports from users, regulators, rights holders, trusted flaggers under Article 22 of the DSA, and other third parties. The team conducts regular audits, validates flagged content, monitors detection systems, and continuously updates policies in line with regulatory developments and emerging risks. Furthermore, content moderators receive training on Product Compliance, IP, and Content Compliance, which is supplemented by regular coaching and case reviews. Multilingual specialists across EU markets provide enforcement support tailored to local requirements. This framework enables Temu to ensure the timely removal of non-compliant content, protect IP rights, and maintain marketplace safety and reliability. The table below summarises the mitigation measures assessed for effectiveness across individual sub-modules.

Risk category	GRC Control Descriptions
Product Compliance	**Risk intelligence**: Whaleco manages product compliance risks on Temu through risk intelligence that incorporates regulatory guidance, internal enforcement data, media monitoring, and stakeholder feedback. The TST conducts regular intelligence reviews to anticipate emerging risks and identify systemic vulnerabilities. Where gaps are identified, root-cause analyses drive corrective action and guide the prioritisation of future controls. **Inspector oversight and mock cases**: To validate the effectiveness of safeguards, Whaleco engages experienced inspectors to conduct targeted reviews of product listings and embeds mock cases within moderator workflows to assess judgment accuracy and consistency. These mechanisms ensure that Product Compliance risks remain closely monitored and effectively managed.

Risk category	GRC Control Descriptions
IP	**Cross-team collaboration**: Whaleco houses dedicated teams covering six core IP functions: IP legal, proactive monitoring, rights holder collaboration, trader qualification review, global IP coordination, and quality development. These teams collaborate closely to maintain cohesive IP risk management. For example, the proactive monitoring team incorporates insights from rights holder collaboration and IP legal teams to refine brand control lists and enhance targeted enforcement. Meanwhile, the rights holder collaboration team provides updates on rights holders' IP assets and enforcement priorities, enabling the proactive monitoring team to align its detection strategies with brand-specific needs. Regular cross-team case reviews strengthen this collaborative approach. **IP policy framework**: Temu's IP policy framework is implemented through standardised internal guidelines that set out responsibilities for IP risk management, including identifying alleged infringements and promptly removing IP infringing listings. **IP enforcement**: Leveraging the policy framework, Whaleco implements consistent, scalable enforcement that combines automated detection with human review and balances precision and efficiency in removing infringing product listings. During the Relevant Period, this approach has earned positive recognition from rights holders and industry associations. Additionally, dedicated teams monitor external feedback and conduct prompt follow-ups to address concerns or mitigate the risks, creating a continuous feedback loop that strengthens detection strategies and overall IP protection effectiveness.
Content Compliance	**Limited UGC functionalities minimising content compliance risks**: Temu is an online marketplace, not a social platform. User-generated content is restricted to the following limited scenarios, apart from trader-generated product listings: (i) Product reviews submitted by consumers who purchased relevant products; and (ii) Trader-consumer chat functions initiated solely by the consumer regarding specific orders. This focused approach to UGC allows Temu to maintain a commerce-focused environment while mitigating content-related compliance risks.

ii. Mitigation measures relating to Policies & Standards

Whaleco mandates that all traders execute a Seller EU Services Agreement prior to onboarding. The agreement governs traders' access to and use of Temu services and incorporates additional binding requirements, including the Temu Product Safety and Compliance Policy (which covers IP), the EU Seller Code of Conduct, and other rules, specifications and policies published in the Temu EU Seller Center (together, the "Temu EU Seller Rules"). Under the Seller EU Services Agreement and the Temu EU Seller Rules, traders must ensure that their products and listings are authentic, lawful, and compliant with platform policies, and must not list prohibited or non-compliant items. Traders are notified of the consequences of infringements and may be required to produce documentary proof of product authenticity or safety on request. Similarly, users are bound by Temu's Terms of Use, which

prohibit submissions (including reviews and uploads) that infringe third-party rights or contain harmful, discriminatory, or otherwise objectionable content. Collectively, these contractual terms constitute binding safeguards by obligating both traders and users to refrain from listing or sharing infringing, unsafe, or non-compliant content on Temu.

The table below summarises the mitigation measures assessed for effectiveness across individual sub-modules.

Risk category	Control Descriptions: Policies & Standards
Product Compliance	Whaleco's Product Compliance framework adapts to and aligns with evolving regulations and business objectives. At its core is the Product Safety and Compliance Policy, which defines prohibited product categories, identifies products subject to safety requirements, and references the applicable legislation across the EU Member States. Whaleco's policy development team plays a key role in keeping these standards current. This working group within the TST comprises legal professionals, e-commerce specialists, and subject-matter experts. To further strengthen the precision of Whaleco's regulatory interpretations, the team collaborates closely with external advisors and integrates their specialised insights and guidance into Whaleco's policy framework.
IP	Whaleco requires third-party traders and users to comply with a comprehensive set of contractual obligations and policies designed to prevent the posting of IP-infringing content from the outset. Central to this framework are binding instruments for traders and users, including the Seller EU Services Agreement, Seller Code of Conduct, Intellectual Property Policy, and the Terms of Use for Temu users. Together, these instruments define infringing conduct, establish enforcement procedures, and specify the consequences of violations. Whaleco's IP legal team ensures that these standards remain current with evolving regulations and industry best practices. To enhance the precision and relevance of the framework, the team collaborates closely with external advisors and IP rights holders to incorporate specialised insights into policy updates and enforcement guidance. This adaptive approach enables Whaleco to maintain a first line of defence against IP infringement by contractually obligating traders and consumers to refrain from posting infringing content, while underpinning proactive monitoring and responsive enforcement across Temu.
Content Compliance	To mitigate Content Compliance risks presented by Temu's limited UGC scenarios, Whaleco has implemented a dedicated set of policies governing the use of Temu's services. Core policies include Temu's Terms of Use, Community Guidelines, and Review Guidelines. Together, these documents expressly prohibit illegal or harmful content such as hate speech, profanity, obscene language, and any other content deemed offensive, objectionable, or abusive. These policies are regularly reviewed and updated by Whaleco's LCT to ensure they uphold platform integrity and meet evolving regulatory requirements, without compromising user rights. All policies are accessible

Risk category	Control Descriptions: Policies & Standards
	by the public on Temu, and Whaleco communicates material updates to keep users informed.

The following case study highlights the practical outcomes and effectiveness of the GPSR compliance.

Case Study: GPSR Compliance

In alignment with the GPSR, Whaleco operates Temu as a consumer-oriented platform with a strong commitment to product safety and regulatory compliance. Whaleco promptly removes illegal or unsafe products identified through proactive monitoring, consumer notifications, or regulatory communications, and undertakes appropriate follow-up measures, including performing recalls, and publishing recall-related information.

To ensure transparency and traceability, Whaleco collects and publicly displays on Temu the following product-related information:

- EU Responsible Person details
- manufacturer information
- product identification number
- trader information
- multilingual safety warnings in accordance with the GPSR or other applicable Union harmonisation legislation

In addition, trader training materials are regularly updated to reflect emerging trends and reinforce compliance obligations. Prior to GPSR enforcement, Whaleco issued multiple guidelines and designed specific training sessions to assist traders fully understand the forthcoming legal obligations and the steps necessary to achieve compliance. Products that failed to comply with such guidance were removed from Temu, and traders were only permitted to resume offering products to EU consumers once they had submitted the required documentation and demonstrated compliance.

Through dedicated training and advance notice, the majority of the traders were well-prepared and cooperative in this consumer-centric initiative. [Confidential]

iii. Mitigation measures relating to User Management & Onboarding Control

Temu have established a rigorous trader onboarding and vetting system designed to ensure compliance and credibility from the outset. [Confidential] Upon receiving a trader's application, Whaleco cross-verified the information provided against official third-party databases to confirm the accuracy and completeness of necessary details, including company name, registration number, legal representative, and operating status. To further prevent malicious actors from registering with Temu or reapplying under new identities, Whaleco maintains a trader blocklist ("**Trader Blocklist**"), which effectively blocks high-risk traders on government-issued sanctions lists and entities related to previously suspended bad actors from re-entering Temu.

Following onboarding, Whaleco implements continuous monitoring and trader education measures to ensure sustained compliance. The platform systematically and regularly reviews trader information to ensure it is accurate and up to date. When changes occur or key details approach expiration, traders are notified and required to update their records accordingly. Failure to do so results in enforcement actions, including suspension of their ability to sell to the EU market. During the Relevant Period, Whaleco issued over 43,000 notifications to traders requesting updates or additional information on

their products due to the impending expiration of information or registration certificates. Where traders failed to update the relevant materials by the expiration date of their information or registration certificates, Whaleco would immediately suspend their ability to sell products on Temu. [Confidential]

Complementing its enforcement framework, Whaleco operates a dedicated online Seller Education Programme, which has attracted significant engagement, generating over 8 million views during the Relevant Period. In addition to self-learning resources, Whaleco delivers structured capacity-building initiatives, including a recurring monthly training series organised in partnership with the EU consumer protection organisation SPEAC, designed to further strengthen traders' compliance awareness. Meanwhile, to support traders in strengthening compliance while reducing associated costs, Whaleco provides a compliance service hub. This portal connects traders with a wide pool of certified third-party service providers, helping ensure that their products meet applicable EU standards and labelling requirements. By facilitating accurate matching with suitable services, it enables traders to lower search and coordination costs. Importantly, the hub serves solely as an informational resource, allowing traders to make independent choices. All transactions are redirected to the service providers' own websites, and Whaleco remains fully independent from the providers.

These concerted efforts have helped foster a high-quality trader community on Temu. According to internal data, storefronts with a consumer rating of [Confidential] of Temu's total orders during the Relevant Period. This indicates that the majority of transactions are handled by top-rated traders.

The table below summarises the mitigation measures assessed for effectiveness across individual sub-modules.

Risk category	Control Descriptions: User Management & Onboarding Control
Product Compliance	**Qualification requirements**: For Product Compliance, Whaleco enforces strict category-specific qualification requirements. Before listing products, traders must upload the necessary compliance documentation corresponding to the product. For example, food traders are required to provide verified Hazard Analysis and Critical Control Point ("**HACCP**") Certificate or equivalent certifications, which are cross-checked against official records before approval to sell is granted. Other categories may require documents such as CE marking, test reports, or compliance labelling. These qualification requirements are dynamically updated in line with EU and Member State legislation to ensure ongoing compliance. **Automated and human review**: All uploaded certification materials are first subject to automated review to verify completeness and basic compliance. Where automated systems cannot reach a conclusive determination, cases are escalated to Whaleco's human review team for further assessment.
IP	**IP Verification Requirement:** Whaleco enforces IP verification requirements before branded products can be listed. Traders must submit valid brand authorisation documents or purchase invoices. These materials undergo two rounds of human review, with a third-level adjudication applied in cases of discrepancy. Reviewer accuracy is monitored through daily quality assurance checks conducted by an external quality assurance (QA) team Branded products cannot be published until the associated IP documentation has been verified. Traders providing incomplete or invalid documents will be asked to submit supplementary materials.

Risk category	Control Descriptions: User Management & Onboarding Control
	Controls on Document Compliance and Expiry: Submission of non-compliant documents may result in a Level 3 suspension (account suspension and removal of all product listings). If non-compliant IP credentials are identified through external feedback or internal checks, Temu promptly initiates an investigation, and once the documentation is confirmed to be non-compliant, it will lead to penalties. To further ensure compliance, Temu operates an automated monitoring system that checks document validity on a daily basis, sends automated reminders 30 days and 7 days prior to expiry, and automatically delists affected branded products from the trader's store on the date of expiry until updated authorisation documents are submitted and successfully verified. **Trader Education:** Trader education complements these procedural safeguards. Through the Seller Education Programme, over 90 dedicated IP compliance courses are available, covering topics such as brand awareness, trademark use, and documentation requirements.

iv. Mitigation measures relating to Detection & Enforcement

Whaleco has established a unified content moderation framework that integrates automated detection with professional human review. [Confidential] At the operational level, automated detection systems perform large-scale screening of listing data, while complex or ambiguous cases are escalated to a dedicated team of trained reviewers for manual assessment. This hybrid approach functions as a self-improving closed-loop system: continuous feedback from regulators, rights holders, trusted flaggers, and global monitoring sources informs the refinement of both detection models and enforcement rules. Additionally, Temu conducts annual automated system audits to validate and optimise performance. As indicated in Temu's latest transparency report, the automated detection precision, accuracy, and recall rates for content moderation reached 99.98%, 99.88%, and 79.40% respectively. During the Relevant Period, Temu's moderation system proactively intercepted and removed approximately 140 million potentially non-compliant product listings and potentially IP infringing products. This demonstrates both the scale and effectiveness of Temu's controls in reducing recipients' exposure to infringing or unsafe products.

In addition to proactive detection, Whaleco is committed to working with EU recipients of the service, regulatory authorities, rights holders and other stakeholders to maintain a compliant and secure Temu marketplace. Whaleco provides all recipients with the opportunity to report potentially illegal content on Temu. All reports are assigned to dedicated teams for handling and are continuously used to optimise the content moderation systems, thereby achieving a positive feedback loop.

The table below summarises the mitigation measures assessed for effectiveness across individual sub-modules.

Risk category	Control Descriptions: Detection & Enforcement
Product Compliance	**Proactive Controls** Whaleco has built a Product Compliance framework that integrates automated detection with human review. Supplemented by additional measures such as cross-check and spot audits, this framework forms a unified and cohesive ecosystem, managing Product Compliance across pre- and post-listing stages. Before listing, text and image recognition technologies are applied to screen products, automatically detecting missing or inconsistent documentation,

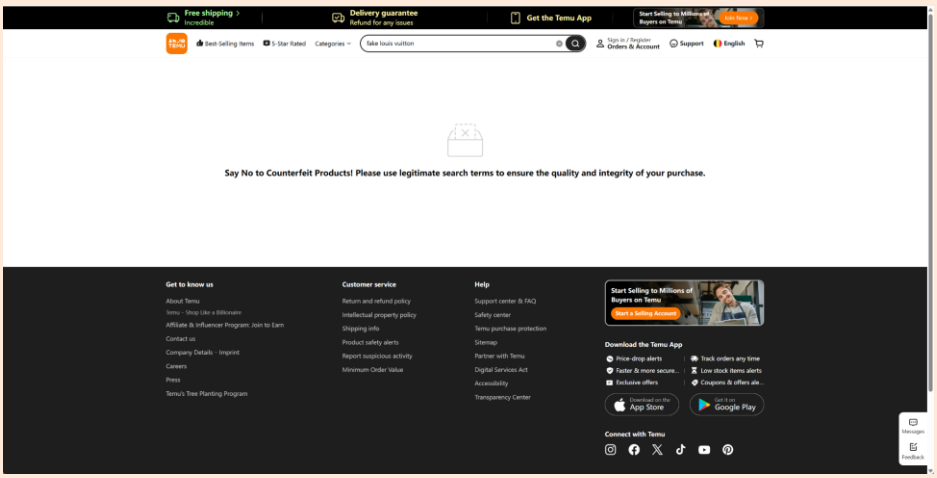
Risk category	Control Descriptions: Detection & Enforcement
	prohibited keywords, and previously identified non-compliant products. Automated systems are subject to accuracy testing and periodic audits to maintain reliability. Products that cannot be conclusively assessed by automated systems are escalated to a professional review team to ensure compliance with EU regulatory requirements. After listing, the system continuously learns from regulatory orders, user feedback, and enforcement outcomes, forming a closed-loop process of self-optimisation that strengthens detection capabilities and enables rapid responses to emerging risks. Complementing this, the cross-check mechanism applies these enhanced capabilities in its ongoing screening, utilising intelligence from various channels to systematically identify and remove product listings that are identical or substantially similar to known non-compliant items. Supported by this dual-layer review mechanism, Whaleco proactively intercepted and removed over 103 million potentially non-compliant products during the Relevant Period, accounting for approximately 99.99% of all product listings removed. Only 0.01% were removed in response to external feedback, underscoring the effectiveness and reliability of Temu's proactive moderation mechanism. Of all removals, 80.90% were results of automated processing while 19.10% were driven by human reviewers. **Reactive Enforcement Mechanism** In addition to proactive moderation, Whaleco operates extensive tools to address Product Compliance issues reported through external channels. This includes a **"Report this item"** feature on Temu, a single point of contact for market surveillance authorities, and other external feedback channels. All reports submitted through the "Report this item" channel are transmitted to Temu's moderation system, where trained content moderators verify reported issues and assess potential non-compliance against internal policies. Verified non-compliant items are immediately removed, and the cross-check mechanism is triggered to identify and remove identical or materially similar products. During the Relevant Period, Temu received over 73,000 notices through this channel, with an approximately median response time of 16 hours. Further, to the extent a report is dismissed, and the reporter is dissatisfied with the platform's decision, affected reporters can easily initiate an appeal through the decision notification. During the Relevant Period, 65 cases in which the notices were originally dismissed were subsequently overturned and upheld following reporters' appeals. In line with Article 22 of the DSA and to the extent any such report is submitted, Temu prioritises reports from trusted flaggers—certified entities registered through Temu using official emails. Reports submitted by trusted flaggers are expedited for immediate review, ensuring rapid action on high-risk Product Compliance issues. During the Relevant Period, no trusted flagger reports concerning Product Compliance were received. Whaleco also collaborates with EU Member States' regulatory authorities. Upon receiving regulatory notifications, the TST takes immediate actions, including takedowns, cross-checks, and updates to internal policies, procedures, and trader guidance to prevent recurrence. During the Relevant Period, about 180

Risk category	Control Descriptions: Detection & Enforcement
	regulatory notices led to the removal of about 560 potentially illegal or non-compliant product listings, with a median response time of 15 hours. This reactive framework complements proactive measures, ensuring rapid identification and removal of non-compliant products while strengthening Temu's overall compliance ecosystem. **Correction of Misplaced Product Categories** To prevent traders from misplacing product listings, whether accidentally or deliberately to circumvent category-specific rules, Whaleco employs robust moderation tools. Automated screening analyses product descriptions and images to predict the appropriate product category and flag discrepancies between the predicted category and the trader's placement. Cases where the system cannot make a conclusive determination are escalated for manual review. [Confidential] Based on Whaleco's observations, most cases involved harmless misplacements. This typically occurred either because traders misinterpreted categories due to cognitive errors, or because the products themselves had an inherently ambiguous nature, making them legitimately suitable for multiple scenarios. For example, an outdoor camping table could be incorrectly listed as a home dining table. [Confidential] **Physical Spot Checks** Whaleco conducts daily spot checks on physical products by using a combination of independent, accredited laboratory testing and eye-check inspections performed by experienced inspectors. [Confidential] To ensure authoritative testing and recognition across jurisdictions, Whaleco partners with highly reputable third-party laboratories selected for their accreditations (ISO 9001, ISO 14001, ISO/IEC 17025) and industry reputation. In April 2025, Whaleco partnered with Eurofins Consumer Product Testing to cover toys, textiles, electronics and furniture[2], which further deepens Whaleco's existing testing capabilities for these key areas. Earlier that year, Whaleco also teamed with TÜV SÜD, TÜV Rheinland Group, SGS and Bureau Veritas Group to reinforce worldwide compliance standards. Laboratories are staffed by qualified personnel trained in category-specific standards, including toy safety (EN 71), cosmetics (EN ISO 22716:2007), and other general product safety requirements. For products listed across multiple jurisdictions, separate tests are conducted to verify compliance with local regulatory standards. These laboratories also support Whaleco's internal compliance knowledge through training and guidance. In parallel, Whaleco engages external inspectors to perform impartial visual inspections. Inspectors follow detailed operational manuals tailored to each product category. Physical and mechanical tests are conducted to evaluate durability, functionality, and compliance, including product authenticity, safety regulation adherence, newness, correct labelling, and proper packaging.

[2] Accessible at: https://www.prnewswire.com/news-releases/temu-strengthens-commitment-to-quality-assurance-with-eurofins-consumer-products-testing-partnership-302421796.html.

Risk category	Control Descriptions: Detection & Enforcement
	Spot checks serve as a critical physical safeguard, complementing digital controls to guarantee end-to-end product safety and integrity.
IP	**Rigorous Proactive Controls** Whaleco has established a layered detection system combining automated detection with human review to provide comprehensive IP protection across pre- and post-listing phases. [Confidential] At the pre-listing phase, all product information provided by traders undergoes automated screening. The system automatically flags and blocks product listings that may infringe on IP rights, while ambiguous cases are escalated to well-trained reviewers, who receive regular training to ensure consistent and accurate enforcement decisions, for further review. During the Relevant Period, over 22 million product listings were blocked due to IP infringements in the pre-listing phase, demonstrating the system's ability to intercept risks before product listings go live. At the post-listing phase, the automated system continues to monitor products in real-time and apply the same processes described above. The underlying detection models are developed with the support of training data annotation. Image recognition plays a critical role in the detection process, particularly for identifying subtle or modified brand marks within product images. This requires high-precision, high-coverage annotation to ensure accurate model performance. The human review team is organised by brand or rights holder, with specialised personnel responsible for specific brand or IP portfolios. This structure enables reviewers to develop deep expertise in relevant IP assets, ensuring more accurate and reliable enforcement decisions. They validate or overturn automated results, resolve ambiguous cases, and label IP infringements. These labelled cases are fed back into the system to refine detection rules and enhance automated detection, creating a closed-loop optimisation that continuously improves accuracy and reduces false positives. During the Relevant Period, Whaleco proactively removed around 38 million products for potential IP infringements. In comparison, only about 122,000 products were removed in response to third-party reports submitted through the IP Portal, Brand Registry Portal, or the "Report this item" function [Confidential], underscoring the effectiveness of proactive measures in intercepting IP risks. [Confidential] **2. Reactive Enforcement Mechanism** In accordance with DSA requirements, Temu provides robust notice-and-action mechanisms for rights holders and users to report suspected IP infringements. These mechanisms enable them to submit and manage complaints efficiently, with clear escalation and withdrawal procedures. **(1) IP Portal** Temu's dedicated IP Portal allows rights holders to report alleged IP infringements on Temu for all types of IP rights, including copyrights, trademarks, patents, design rights, and applicable unregistered rights. Since the launch of IP Portal in September 2023, Temu has raised the submission limit per report from 50 to 200 URLs to better support rights holders. Rights holders can

Risk category	Control Descriptions: Detection & Enforcement
	track the status of their submissions through a centralised complaint tracking system. To streamline the process, Whaleco has introduced a one-click feature that automatically populates related fields when submitting IP reports for previously referenced rights, reducing the need to resubmit the same documents multiple times. During the Relevant Period, Temu received over 73,000 reports from rights holders. These were processed within a median response time of 24 hours, with takedown rates as follows: • Design: 73.35% • Trademark：73.25% • Copyright：55.21% • Patent：33.70% All reports are reviewed by specialised personnel, and submissions from trusted flaggers are prioritised for timely handling. During the Relevant Period, Temu received seven reports on IP infringements from trusted flaggers, all of which were processed expeditiously. To ensure timely and appropriate review, a notification mechanism has been established to alert reviewers upon receipt of a trusted flagger report, ensuring it receives priority attention during the review process. **(2) Brand Registry Portal** In December 2023, Temu introduced the Brand Registry Portal to strengthen reporting for trademarks. Rights holders can securely store their trademark information and submit takedown notices without repeatedly providing supporting documents. During the Relevant Period, over 600 trademarks were stored, and around 3,500 reports were submitted via the Brand Registry Portal, with a median response time of 19 hours, among which 76.29% resulted in takedown actions. Rights holders can efficiently monitor and manage all complaints, ensuring enforcement. Since July 2025, the Brand Registry Portal has also supported the submission of copyright complaints, further expanding the scope of the Brand Registry Portal. **(3) Report this item** Whaleco also provides an efficient user reporting channel on Temu's online interface. Users can report suspected counterfeit and infringing products through the "Report this item" function on the product page. Each user report is manually reviewed by a dedicated team, and once verified, appropriate enforcement actions are taken promptly to maintain an orderly marketplace. During the Relevant Period, Whaleco received approximately 4,000 IP-related reports through this function, which were processed within a median response time of about 18 hours, with 27.47% resulting in takedown actions. **(4) Consumer Awareness Notification** Whaleco recognises that effectively combating counterfeit products requires engaging and informing consumers. Consumers play a crucial role in reducing demand by understanding the risks of counterfeit products and the value of authentic items. To support this, Temu has added alerts within search results that appear when users enter search terms associated with counterfeit products. These messages provide real-time guidance to promote informed purchasing decisions and

Risk category	Control Descriptions: Detection & Enforcement
	protect brands. A recent daily snapshot shows that the alerts were triggered more than 12,000 times, helping users distinguish between genuine and counterfeit products. 
Content Compliance	As outlined in **Section IV**, Temu limits user-generated content to protect platform integrity: only consumers who purchased relevant products can post reviews on the product listing page or use the chat function to contact traders for order-related questions. Traders cannot proactively contact users. These preventative designs significantly reduce content compliance risks. Complementing this, Whaleco's governance framework includes a comprehensive set of Policies & Standards, grounded in the Terms of Use, Community Guidelines, and Review Guidelines, which strictly prohibit illegal or harmful content, including hate speech, obscenity, misinformation, and abusive behaviour. To further reinforce compliance, Whaleco intercepts external links often used to bypass platform controls. To implement these rules effectively, Whaleco operates a technology-driven moderation framework that combines automated detection with expert human review. Automated moderation system screens product listings and descriptions for enforcement on non-compliant content, while ambiguous cases are escalated to human reviewers. For complex content like multilingual text or content embedded in images and videos, Whaleco employs high-accuracy machine translation and conducts cross-check with its moderation system to help detect difficult-to-find violations. This multi-layered approach enables comprehensive enforcement across diverse content types. During the Relevant Period, over 89,000 non-compliant contents from the review function were proactively removed. Whaleco also empowers users to play an active role in maintaining platform compliance through the "Report this review" feature. During the Relevant Period, over 6,600 notices of reviews violations were submitted; approximately 400 resulted in takedown actions, with an average takedown time of 11 hours.

v. Mitigation Measures relating to User Rights and Redress Mechanisms

Trust and Transparency are the foundation of a thriving Temu community. Guided by this principle, Whaleco strives to protect every voice by conducting careful reviews of each case to ensure users' freedom of expression is always upheld. A key indicator of product safety and conformity outcomes is

the post-sale dispute rate, which reflects cases where consumers report dissatisfaction with the products received for any reason (e.g., mismatch with the listing, unmet expectations, or quality concerns). [Confidential]

With this commitment at the core, Whaleco has established clear and accessible feedback and complaint channels, ensuring every user (including traders) affected by Whaleco's decisions has a direct avenue to be heard. Each appeal undergoes thorough review and deliberation by Whaleco's experienced and professional reviewers to ensure fair and impartial outcomes. Whaleco provides a clear SOR for affected users, with the option to seek redress through out-of-court dispute settlement mechanisms referred to in Article 21 of the DSA.

Whaleco recognises that even robust safeguards cannot prevent every potential compliance risk. To address this, Whaleco has established extensive remedial channels to mitigate potential harm to its consumers. A key component of these efforts is Whaleco's product recall process. When a recall is initiated, Whaleco promptly removes affected products from sale, notifies impacted consumers on behalf of traders, and issues automatic refunds through the original payment channels.

The table below summarises the mitigation measures assessed for effectiveness across individual sub-modules.

Risk category	Control Descriptions: User Rights and Remedies Mechanisms
Product Compliance	Whaleco fully respects the fundamental rights of all EU users. When restrictive measures are imposed on traders for violation of Product Compliance-related policies, Temu issues a statement of reasons that includes the information required under Article 17(3)(a)–(f) of the DSA to the affected trader. This measure is designed to help traders understand the grounds and legal basis for the enforcement action, thereby reducing the risk of repeated infringements of Temu rules or applicable laws and regulations due to legal unawareness. Whaleco places particular emphasis on informing traders, within the statement of reasons, of the available possibilities for redress, including Temu's internal appeals mechanism, out-of-court dispute settlement referred to in Article 21 of the DSA. All appeals submitted, supplemented by supporting documentation if any, are assigned to a dedicated review team to ensure timely and accurate assessments. When an appeal is upheld, Whaleco promptly restores the user's position to its state prior to the enforcement action. During the Relevant Period, Temu received over 107,000 appeals relating to restrictive measures imposed under the product compliance-related policies. The median appeal response time was approximately four days, and the appeal success rate was 30.70%. **Product Recall Procedure** To safeguard consumer rights, Temu works closely with regulatory authorities and traders to implement product recalls. The TST promptly processes recall notifications from regulators and takes the following actions: • Remove recalled products and cross-check to eliminate similar product listings on Temu • Forward recall notices to traders together with a detailed statement of reasons in line with Article 17 of the DSA

Risk category	Control Descriptions: User Rights and Remedies Mechanisms
	• Require traders, under the Seller EU Services Agreement, to carry out recalls and report to regulators • Notify consumers with product details (including name, brand, batch or serial number, images where applicable, and other relevant identifiers) • Ensure all affected consumers receive full refunds within a reasonable timeframe • Publish recall information on the "Product Safety Alerts" page for public visibility • Provide continuous guidance to traders to ensure compliance with applicable laws and regulations Temu's recall mechanism emphasises transparency and timely reporting. Once a recall is triggered, Whaleco provides regulators with detailed reports on the recall process and reasons, while monitoring each stage to ensure timely execution and compliance with standard procedures. Although regulators generally require remedial actions within two business days, Temu prioritises consumer safety and typically initiates recall procedures within one business day of receiving a notice. In addition to direct email notifications sent to affected consumers, a clear and prominent recall notice is published on the Temu "Product Safety Alerts" webpage for public visibility and information. [Confidential]
IP	Whaleco recognises the importance of fair and transparent recourse for all, including rights holders, users, and traders. To uphold this principle, Whaleco provides a structured appeals and correction mechanism for IP-related matters. Rights holders, users and traders may submit appeals to challenge decisions or correct issues identified during the IP review process. The appeals process allows reporters to submit supporting evidence to demonstrate non-infringement or to correct and/or supplement reported issues, based on clear criteria such as content rectification, documentation verification, and identification of wrongful removal. During the Relevant Period, Whaleco received over 3,000 trader appeals against IP takedown decisions. By the end of Relevant Period, appeals were processed with an average response time of 48 hours. [Confidential] While appeals from rights holders and users are channelled through the IP reporting interfaces (e.g., IP Portal, Brand Registry Portal and Report this item), these submissions are subject to manual verification and feedback, enabling appropriate adjustments or reaffirmation of initial decisions based on supplementary materials or clarifications submitted. They may also withdraw submitted reports if the information is inaccurate, ensuring the review process remains accurate, fair, and transparent. In addition to appeals and report withdrawal, Whaleco provides remedial measures for consumers affected by IP infringements. During the Relevant Period, the refund rate for purchases of IP infringing products reached 94.25%, with a median after-sales handling time of under one minute.

Risk category	Control Descriptions: User Rights and Remedies Mechanisms
	These mechanisms ensure fair, impartial resolution for all parties affected by IP enforcement actions, enhancing transparency, accountability, and trust in Temu's IP dispute process
Content Compliance	All users subject to restrictive measures for infringements of Temu's content compliance policies receive SORs containing the information required under Article 17(3)(a)–(f) of the DSA. SORs contain details on available appeal channels and other possibilities of redress. During the Relevant Period, Whaleco received over 3,300 appeals against review-moderation decisions based on Community Guideline violations. Of these, [Confidential] were overturned, with a median response time of about 19 hours.

vi. Mitigation measures relating to External Engagement

Whaleco maintains structured and ongoing collaboration with regulators, industry associations, and rights holders to enhance compliance in areas including Product Compliance, IP, and Content Compliance. This cooperation takes shape through formal partnerships, involvement in multi-stakeholder initiatives, and consistent dialogue at both national and international levels. Insights and feedback from such engagement are integrated into Whaleco's compliance framework, facilitating continuous improvement and ensuring adherence to evolving regulatory standards and industry best practices.

The table below summarises the mitigation measures assessed for effectiveness across individual sub-modules.

Risk category	Control Descriptions: External Engagement
Product Compliance	As Temu's community of traders and users expands, Whaleco faces increasing responsibilities and challenges. Public discourse surrounding e-commerce platforms like Temu continues to intensify, and Whaleco recognises that building a marketplace for long-term success requires embracing these dialogues and listening carefully to diverse perspectives so as to learn and transform them into tangible improvement. Guided by this purpose, Whaleco has strengthened its force to navigate and respond to the external landscape. This includes actively tracking and integrating external regulatory intelligence from the EU and EU Member States authorities, consumer organisations, and official databases such as RAPEX, RASFF, OECD Global Recalls, and national recall portals. Daily updates from these sources are integrated into Whaleco's moderation systems to enhance detection capabilities. Complementing this, a dedicated team monitors hundreds of EU media outlets to capture early signals of potential product safety concerns. Following the principle that prioritises product safety, when potentially non-compliant products are identified on Temu, Whaleco removes them pre-emptively while ensuring that traders are granted the opportunity to appeal, thereby preventing the potential dissemination of illegal products. This dual reliance on official intelligence and proactive media monitoring enables Whaleco to respond swiftly, strengthen safeguards, and mitigate compliance risks at scale. In addition, Whaleco actively engages with external authorities to address product compliance issues and strengthen platform governance. This engagement takes place through bilateral dialogue and correspondence,

Risk category	Control Descriptions: External Engagement
	such as exchanges with the Australian Competition and Consumer Commission (ACCC), and the UK Office for Product Safety and Standards (OPSS), where targeted control measures are discussed and opportunities for collaboration on product safety and consumer protection are explored. All such interactions have yielded constructive and positive feedback, which Whaleco incorporates to continuously refine its control measures. For example, the Swedish Chemicals Agency (KEMI) confirmed in writing that its recent product sampling test found no restricted substances exceeding REACH thresholds. Taken together, this combination of regulatory collaboration and constructive external feedback helps Whaleco advance its governance framework and contributes to building a trusted and safe online shopping environment for EU users. **Cooperation with SPEAC** Whaleco has established a structured collaboration with the EU-funded SPEAC (Safe Non-Food Consumer Products in the EU and China) project to enhance trader compliance and product safety awareness. Training needs are systematically identified based on regulatory updates, trader feedback, and compliance risks flagged by regulators. The training content is developed with expert input from SPEAC and delivered through online sessions that combine specialist presentations with interactive Q&As to address trader concerns. In addition, Whaleco leverages SPEAC's resources to stay informed about regulatory developments and emerging product risks. For instance, recent alerts on infant carrier safety prompted updated compliance guidance, while a joint training held in June 2025 on electrical products provided insights into unsafe items notified via the EU Safety Gate portal. By embedding SPEAC expertise into its compliance framework and driving high levels of trader participation, Whaleco has enhanced both trader awareness and the overall safety and reliability of products on Temu. **Participation in Conferences, Seminars, and Workshops** Whaleco actively participates in conferences, seminars, and workshops covering a broad range of topics relevant to the e-commerce industry. Insights and information gathered from these events are used to strengthen and refine its compliance infrastructure. For instance, on 10 July 2024, Whaleco participated in a seminar focused on market access and product safety compliance requirements for electronic products in the EU, the US, and Japan. The event, organised in collaboration with leading e-commerce platforms and international certification bodies, addressed topics such as EU market access interpretations, the declaration of conformity, and other key compliance obligations. In addition, Whaleco regularly consults industry specialists regarding product categories that may present higher regulatory risks or safety concerns, including electronics, cosmetics, and toys. Whaleco also participated in the International Consumer Health and Product Safety Conference ("I**CPHSO**") held last year and the OECD forum on combatting illicit trade, which convened in France in February 2025.

Risk category	Control Descriptions: External Engagement
	Collaboration with EU Consumer Association Whaleco values external input and continuously collaborates with third-party organisations across the EU to enhance consumer rights, contributing to a safer and more responsible digital ecosystem for all users. Further strengthening this commitment, Whaleco has established a long-term collaboration with CODICI[3], a respected Italian consumer protection association with over 30 years of experience in safeguarding consumers' rights. Built on shared principles of transparency and accountability, this partnership drives joint monitoring initiatives, annual forums, and dedicated communication channels to address and resolve practical concerns raised by stakeholders. In addition, Whaleco maintains strong communication with EU third-party organisations, jointly providing guidance to foster a trusted and safe shopping community.
IP	Whaleco operates a dedicated Brand Collaboration function within its compliance framework to safeguard IP rights on Temu. Collaboration with rights holders is central to this effort: As of August 2025, Whaleco engaged directly with over 2,000 brands and maintained ongoing dialogue with 70 industry associations, fostering constructive feedback and supporting broader IP enforcement initiatives. Each brand is supported by a designated liaison for case-specific assistance and escalation, with ad-hoc task groups convened as needed for complex matters. **Brand Guardian Initiative** Launched in May 2024, the Brand Guardian Initiative provides tailored support for rights holders with complex IP portfolios or unique enforcement challenges. Participating brands work directly with Whaleco to catalogue and validate their IP assets, which are then integrated into proactive monitoring technologies to enhance detection precision. The programme also establishes structured communication channels to review brand-specific enforcement priorities and risk patterns. As of August 2025, around 1,500 brands were enrolled, and over 400 IP-asset datasets from these brands enrolled were integrated into monitoring tools. **Industry Engagement** Whaleco maintains structured engagement with international and regional industry associations and rights-holder organisations to strengthen IP enforcement and anti-counterfeiting efforts. Whaleco collaborates with the International Anti-Counterfeiting Coalition (IACC), hosting roundtables in 2024 and 2025 and participating in the Marketplace Advisory Council. As a member of International Trademark Association (INTA), Whaleco participated in Anti-Counterfeiting and Legislative Committees, hosted roundtables at annual conferences, and conducted a webinar for the Online Takedown Procedures Certificate Programme. Whaleco also engages with the Intellectual Property Owners Association (IPO) through its Anti-Counterfeiting, Anti-Piracy, and Copyright Committees. At the European level, Whaleco maintains an ongoing partnership with UNIFAB, participating

[3] Accessible at: https://codici.org/2025/09/15/codici-temu/.

Risk category	Control Descriptions: External Engagement
	in UNIFAB's European Forum of Intellectual Property (FEPI) 2025 and implementing targeted enhancements to its IP tools, including EU-wide takedown jurisdiction selection, expanded consumer education keyword triggers, and automated documentation uploads for authorised agencies. Additional sector-specific collaboration includes the Consumer Healthcare Products Association (CHPA) and Automotive Anti-Counterfeiting Council (A2C2) to address counterfeit product safety risks. Such engagement ensures alignment with industry best practices, reinforces proactive and reactive IP enforcement, and supports regulatory compliance across multiple jurisdictions. A non-exhaustive list of collaborating organisations is provided in Temu's 2025 Intellectual Property Protection Report. **Stakeholder Feedback** As of August 2025, Whaleco received more than 450 positive feedback from over 250 stakeholders, highlighting appreciation for proactive monitoring, timely enforcement actions, and collaborative engagement. Engagement spans diverse sectors, including fashion and luxury, consumer healthcare, electronics, publishing, sports, and creative industries. Representative stakeholder quotes and organisational references are drawn from Temu's 2025 Intellectual Property Protection Report, highlighting the impact of Whaleco's IP enforcement and collaboration initiatives. **Test Purchase Programme** Whaleco conducts Test Purchases in close collaboration with rights holders. This mechanism is specifically designed to verify the authenticity of products suspected of infringing IP rights. In practice, Identification of counterfeit products requires the expertise of the intellectual property rights holder. Inspections are typically initiated in response to consumer complaints, brand requests, or other signals indicating potential infringement. TST procures the identified products and coordinates directly with the respective brands to ensure proper verification and enforcement. [Confidential]

[Confidential]

vii. Other Mitigation Measures Addressing Specific Risk-influencing Factors

In addition to the mitigation measures structured under the defined control domains, Whaleco has implemented dedicated control mechanisms targeting identified risk-influencing factors that could amplify or otherwise impact the platform's exposure to non-compliant content. These measures primarily focus on the recommender systems, the A&I Programme, and controls designed to prevent misuse by rogue traders.

Service & function	Control Descriptions
Recommender system	Built upon Temu's comprehensive content moderation framework, the recommender system synchronises with the platform's dynamic databases of non-compliant products to exclude non-compliant or IP-infringing items from the recommendation pool. Only products that have

Service & function	Control Descriptions
	passed Temu's rigorous pre-listing screening are included in the inventory for recommendation. In the event that a non-compliant product inadvertently evades Temu's initial review but is later detected through Whaleco's continuous screening or extensive external feedback, the recommender system's architecture is designed to promptly capture and address the issue. Once such a product is delisted, it is immediately and automatically removed from all recommendation feeds. Reinstatement occurs only after the product has received full clearance confirming compliance. In addition, for enhanced consumer protection, the recommender system integrates a dedicated tagging protocol managed by the TST to block certain categories of unsuitable content (e.g., adult-only products) from being proactively promoted, whilst these items remain accessible through explicit user search. Specifically, the TST conducts ongoing reviews to identify and tag products that, while not illegal, are inappropriate for broad recommendation. The tagged items are systematically filtered out from proactive recommendations, further safeguarding the user experience.
A&I Programme	Regarding the risk of disseminating non-compliant content through the A&I Programme, it is important to note that the A&I Programme only promotes products that have already been vetted and successfully listed on Temu. No new products are introduced through this channel. All promoted products originate from the same catalogue subject to pre-listing compliance screening and ongoing post-listing monitoring. Accordingly, the A&I Programme does not generate additional compliance risks. The residual risk lies in the possibility that a very small number of non-compliant products, if overlooked during review, may be selected and displayed by Affiliates or Influencers. To address this, Whaleco has implemented a comprehensive set of safeguards. All promoted products remain within Temu's overarching content governance framework, which combines proactive monitoring with external feedback mechanisms to minimise the likelihood of non-compliant items being promoted. These policies, reinforced contractually, include obligations related to truthful promotion and the protection of IP, thereby addressing risks at source. In the rare event that an A&I Programme-promoted product (via links to the product listing page) is later determined to be non-compliant, Whaleco promptly disables the link to prevent further dissemination and subjects off-platform promotional content to ex-post human review. Affiliates or Influencers failing to meet compliance standards are disqualified from earning commissions.
Measure against intentional manipulation by trader	To uphold Temu's compliance standards and prevent misuse by fraudulent users, Whaleco has strengthened its detection and prevention mechanisms targeting non-compliant traders throughout their entire lifecycle on Temu. During onboarding, attempts to gain access through false, duplicate, or incomplete registrations are blocked through the initial vetting process,

Service & function	Control Descriptions
	ensuring only compliant traders join Temu. For onboarded traders, Whaleco conducts continuous checks to verify submitted qualifications and monitor their validity. Traders with expired qualifications and mismatched information, such as a failure to update entity details following registration with the authorities, will be detected through this ongoing scrutiny and get suspended. Services will only be restored after they submit renewed and corrected documentation. In parallel, Whaleco applies a three-tier restriction framework as its overarching penalty scheme, which works alongside its most severe measure - the "Trader Blocklist" - to deter violations and to proportionately penalise offenders based on severity, intent, and frequency of non-compliance. **Three-tier penalty framework** The tiered penalty scheme is structured to promote compliance for traders committing accidental and minor infractions, while reserving the most severe punishment for bad actors exhibiting deliberate malicious intent or persistent violations: **Level 1**: Warning and removal of non-compliant product listings **Level 2**: Suspension of the ability to create new product listings **Level 3**: Account suspension and removal of all product listings **Trader Blocklist** While the three-tier penalty framework serves as an effective safeguard by limiting the ability of non-compliant traders to list products or continue operations, Whaleco additionally maintains a "Trader Blocklist" to ban the most severe offenders - those responsible for egregious violations - from Temu. Once added to the blocklist, the trader's identifiable information, along with information of its affiliated parties, is used to establish tracking criteria. Any future onboarding attempt that matches these details will be automatically intercepted and blocked, prohibiting identified malicious actors from returning to Temu even under a different identity. These measures effectively maintain the integrity of Temu and prevent misuse by bad actors.

D. Residual Risks and Future Mitigation Measures

i. Assessment of Residual Systemic Risk for Illegal Content

Following the review of the inherent systemic risks in relation to dissemination of illegal content and the corresponding mitigation measures, this section assesses the residual risks. Whaleco utilised operational data to compare inherent systemic risks associated with each sub-module against the strength of implemented controls to arrive at the assessment results summarised in the table below.

Sub-Module	Inherent Systemic Risk	Control Strength	Residual Risk
Product Compliance	High (5/5)	Mostly Effective (4/5)	Medium (3/5)

IP	Medium-High (4/5)	Mostly Effective (4/5)	Low-Medium (2/5)
Content Compliance	Medium (3/5)	Mostly Effective (4/5)	Low (1/5)

The assessment that Temu's overall residual risk is maintained at a managed and acceptable level is informed by several key operational characteristics detailed in the preceding "Mitigation Measures" section. A significant factor is the composition of the product catalogue, wherein a substantial proportion of items, by their nature, present a low safety risk (e.g., apparel, textiles, and non-electrical home goods). This composition means that a typical user's exposure is predominantly limited to products with minimal inherent safety concerns. This is complemented by a trader base where a significant majority of all orders are fulfilled by storefronts that have consistently achieved high ratings from consumers. Furthermore, a consistently low post-sale dispute rate serves as an indicator of general consumer satisfaction with the quality and conformity of goods received.

These operational data points align with Temu's residual risk assessment and corroborate its fundamental understanding of the business environment. This understanding confirms that while ongoing governance and mitigation efforts have cultivated a broadly safe and trusted environment for the majority of consumer transactions, product safety risk is distinctly characterised by its potential for severe harm from even a single incident, particularly to vulnerable groups. It is this specific dynamic—a generally safe transactional environment punctuated by the potential for high-impact harm—that logically substantiates the "Medium" residual risk rating for product compliance.

ii. External Intelligence and Regulatory Corroboration

Whaleco cross-validates its residual risk assessment with external perspectives to identify any potentially overlooked significant risks. Findings from external engagement and regulatory monitoring are broadly consistent with Whaleco's internal residual risk findings.

Product Compliance Risk Area

Below are Whaleco's external intelligence and stakeholder engagement efforts in relation to Product Compliance.

Framework for External Intelligence Integration

Continuous Monitoring of Public Information: This involves the proactive monitoring of both official and media sources. Whaleco regularly scans guidance from EU and Member State authorities and continuously ingests data from key international and national recall databases, such as the OECD Global Recalls Portal and the EU's Safety Gate (RAPEX). This is complemented by the systematic monitoring of hundreds of media outlets across the EU. Information gathered is collected daily and integrated into the Temu's moderation systems to enhance automated detection capabilities and trigger prompt internal investigations.

Active Stakeholder Engagement: This pillar reflects a commitment to incorporating industry best practices and expert recommendations. Whaleco maintains an open dialogue through structured channels, including direct consultations with regulators, collaboration with key industry and consumer bodies (e.g., the EU-funded SPEAC project), and ongoing technical exchanges with globally recognised third-party testing agencies, such as TÜV SÜD, Eurofins, Intertek, and Bureau Veritas. Whaleco also actively participates in industry conferences and forums (e.g., the ICPHSO conference and the OECD Forum on Illicit Trade) to exchange insights on emerging compliance risks. Intelligence gathered is systematically assessed and operationalised through timely updates to Temu policies and enforcement procedures.

The analysis of data derived from these methodologies further substantiates the residual risk assessment. As is common for platforms of this scale, Whaleco continuously receives external feedback concerning potentially non-compliant products, both from regulatory authorities and through media reporting. The volume and disposition of regulatory notices are detailed in Temu's periodic transparency reports. All such external intelligence is managed through a structured framework and dedicated processing channels, which also include internal cross-check procedures to ensure thorough mitigation. Notably, the Product Compliance area accounts for a comparatively higher volume of external feedback, a dynamic that is consistent with and factored into its "Medium" residual risk rating.

Despite this volume, Whaleco maintains clear governance objectives focused on constructive engagement and effective resolution. A consistent record of cooperative dialogue with national competent authorities across the EU provides qualitative support for Temu's risk posture. Throughout the reporting period, Whaleco engaged constructively with market surveillance and consumer protection authorities in numerous EU Member States, including Austria, Denmark, Germany, Ireland, Poland, and Sweden. These engagements, which included inquiries on product documentation and potential Safety Gate alerts, were consistently resolved, with all documented cases closed without enforcement action against Whaleco. This record of positive engagement is further evidenced by 11 instances of written correspondence from various EU regulatory bodies acknowledging Whaleco's cooperation and responsiveness. The following case studies illustrate Whaleco's process for promptly acting on regulatory feedback and implementing systemic enhancements:

- **Spain: Proactive Policy Alignment on Common Chargers.** Following communication from the Spanish authority for telecommunications equipment regarding newly transposed national requirements, the TST confirmed that existing internal policies already covered these requirements, as the team had proactively researched and updated them prior to the notification. As a further measure, Whaleco also reinforced its monitoring for this product category.

- **Germany: Systemic Enhancements for CE Marking Compliance.** In response to communications from the German Federal Network Agency (BNetzA) concerning CE marking

issues, Whaleco promptly removed the identified product listings and conducted internal root cause analyses. This led to enhanced internal control mechanisms and updated trader education materials. These efforts resulted in a measurable downward trend in regulatory feedback on CE marking issues, with several months during the Relevant Period recording zero instances.

While Whaleco values feedback from all external sources, including targeted sampling exercises, it is important to contextualise the methodologies involved. Targeted sampling is a valuable tool for identifying potential issues in specific high-risk categories; however, due to its inherent sampling bias, its findings may not be statistically representative of Temu's overall risk profile. Therefore, to provide a more transparent and quantitative assessment of the typical consumer experience, Whaleco is proactively implementing a stratified sampling methodology. This approach will systematically evaluate two core metrics—the Violative View Rate (VVR) and the Violative Order Rate (VOR)—by weighting samples according to the risk level and volume of different product strata. This method offers a more precise and equitable reflection of Temu's safety level and provides a reliable data foundation for ongoing governance efforts.

Intellectual Property Risk Area

In the area of IP protection, the "Low-Medium" residual risk assessment is substantiated by a mature and proactive programme built on deep engagement with rights holders, extending beyond standard notice-and-takedown procedures. A key component of this strategy is the Brand Guardian Initiative, a bespoke programme for rights holders with complex IP portfolios. Since its launch in May 2024, this initiative has enrolled around 1,500 brands and integrated over 400 IP asset datasets directly into proactive monitoring systems. This targeted programme is complemented by broad-scale engagement, including direct collaboration with over 2,000 brands and ongoing dialogue with 70 industry associations. The effectiveness of this collaborative approach is validated by multiple sources. By August 2025, Whaleco has received over 450 instances of positive feedback from over 250 distinct stakeholders. To ensure alignment with global best practices, Whaleco actively participates in leading industry organisations such as the International Anti-Counterfeiting Coalition (IACC), the International Trademark Association (INTA), and the Union des Fabricants (UNIFAB). This deep industry integration and the programme's demonstrable results provide a credible basis for the "Low-Medium" residual risk assessment.

Initiative	Outcome (as of Aug 2025)
Direct Brand Engagement	Over 2,000 brands
Industry Association Dialogue	70 associations
Brand Guardian Initiative Enrolment	Around 1,500 brands
Positive Stakeholder Feedback Instances	450 from 250 stakeholders

[Confidential]

iii. Action Plan for Future Mitigation of Residual Risks

As described above and in line with Article 35(1) of the DSA, Whaleco has put in place reasonable, proportionate, and effective mitigation measures to address systemic risks in relation to non-compliant content, which includes identifying enhancements to these measures. To address the residual risks and potential insufficiencies of the existing mitigation measures identified in the Year 2 risk assessment, Whaleco plans on enhancing the mitigation controls against illegal content risks in the following areas:

Mitigation Type	Description (DSA Article 35)	Controls	Control Enhancement Description
Internal Risk Management & Oversight	Reinforcing the internal processes, resources, testing, documentation, or supervision of any of their activities in particular as regards detection of systemic risk	Product Safety Controls	Whaleco will further expand its product safety controls, including stricter requirements for labelling and other regulated compliance parameters, in addition to the existing mandates for high-risk product categories. Product safety controls will be broadened, building on existing mandates for high-risk product testing (such as for lead, chromium, and nickel content) to include new mandatory data fields and verification processes for labelling and other regulated compliance parameters, such as those anticipated under the Ecodesign for Sustainable Products Regulation (ESPR) and its Digital Product Passport requirement.
Internal Risk Management & Oversight	Reinforcing the internal processes, resources, testing, documentation, or supervision of any of their activities in particular as regards detection of systemic risk	Product Sampling Tests	Whaleco will conduct more frequent and systematic sampling tests of listed products in the prohibited and restricted categories. Whaleco will devote more resources to the current sampling test programme and focus on products in the prohibited and restricted categories. These tests will be carried out by accredited third-party laboratories, with the findings used both for enforcement actions and for improving Temu's content moderation systems. The results will also inform trader education initiatives to prevent recurring violations.
Internal Risk Management & Oversight	Reinforcing the internal processes, resources, testing, documentation, or supervision of any of their activities in particular as regards detection of systemic risk	Proactive External Engagement	Whaleco will strengthen safety control framework by proactively establishing partnerships with product safety regulators and consumer organisations across Europe. Beyond responding to formal notifications, this engagement will include recurring meetings, designated points of contact, streamlined communication, and faster processing of regulatory feedback. This enhanced collaboration will improve the responsiveness and effectiveness of Whaleco's internal controls, ensure closer alignment with regulatory expectations, and reinforce overall product safety across Temu.
Internal Risk Management &	Reinforcing the internal	IP Risk Monitoring	Whaleco will enhance its risk identification mechanisms to address

Mitigation Type	Description (DSA Article 35)	Controls	Control Enhancement Description
Oversight	processes, resources, testing, documentation, or supervision of any of their activities in particular as regards detection of systemic risk		gaps in IP monitoring, particularly for brands not currently covered by its proactive monitoring. Whaleco will broaden the scope of its proactive IP monitoring to include more trademarks.
Internal Risk Management & Oversight	Reinforcing the internal processes, resources, testing, documentation, or supervision of any of their activities in particular as regards detection of systemic risk	IP Intelligence Partnerships	Whaleco will strengthen its IP enforcement framework by partnering with leading IP intelligence firms to provide external verification. Targeting high-risk product categories such as [Confidential], these partnerships will provide independent assessments of infringement risk to complement Whaleco's internal monitoring and risk profiling. This extra layer of external verification will enhance the rigor of enforcement processes, ensure alignment with evolving regulatory expectations, and reinforce overall systemic risk mitigation.
Trusted Flaggers Collaboration	Initiating or adjusting cooperation with trusted flaggers in accordance with Article 22 and the implementation of the decisions of out-of-court dispute settlement bodies pursuant to Article 21	Trusted Flaggers Collaboration	Whaleco will establish closer communication with trusted flaggers, including consumer organisations and regulatory bodies, to strengthen Whaleco's collaborative enforcement framework. Whaleco will proactively reach out to trusted flaggers to strengthen collaboration, including scheduling bilateral meetings to discuss enforcement strategies.

VII. Consumer Protection

This module identifies and assesses the systemic risks in relation to the high level of consumer protection enshrined in Article 38 of the Charter of Fundamental Rights of the EU.

It reflects Whaleco's obligations under the EU consumer protection acquis, specifically the Unfair Commercial Practices Directive ("**UCPD**"), the Consumer Rights Directive ("**CRD**"), the Unfair Contract Terms Directive ("**UCTD**"), and the Price Indication Directive ("**PID**"), which together promote fair commercial practices, transparency, effective dispute resolution, and consumer protection.

In line with Article 34(1)(d) and Recital 83 of the DSA, the module also considers broader societal and individual risks, including gender-based violence, public health, and mental well-being. Risks to physical well-being, which are primarily related to product safety and quality, are addressed separately in the Product Compliance sub-module of **Section VI**, together with IP and Content Compliance. For efficiency, this module focuses on risks arising from inadequate disclosures, misleading practices, and the denial of statutory rights, while risks specifically affecting minors are covered in the Protection of Minors module. Consumer protection, a fundamental right under Article 34(1)(b) and Recital 81 of the DSA, is therefore discussed here without duplicating matters examined in the Fundamental Rights module.

Consistent with the methodology set out in **Section III**, this module identifies inherent systemic risks, evaluates the effectiveness of mitigation measures, and assesses the resulting residual risks. It also outlines design-level protections and supplementary mitigation measures to address risks arising from inappropriate trader conduct. This approach reflects Whaleco's commitment to reducing consumer protection risks both proactively and reactively.

A. 2025 Highlights

From a consumer protection perspective, the systemic risks inherent in operating a platform such as Temu have remained unchanged since the previous year, as such risks are intrinsic to online marketplaces. However, Temu's risk profile has evolved during the Relevant Period in line with its commercial growth. [Confidential]

Whaleco already had in place an extensive array of measures designed to address these risks and provide EU users with the high level of consumer protection to which they are entitled. During the Relevant Period, Whaleco has enhanced these measures in close collaboration with EU regulators.

- In relation to **pricing and promotions**, Whaleco introduced clearer rules for displaying recommended retail prices ("**RRPs**"). Temu now ensures that any RRP displayed is always accompanied by a clear abbreviation and explanatory note, accessible through multiple points (e.g., hovering over the price, the "RRP" text, or a "(?)" icon). [Confidential]

- In relation to **consumer rights**, Whaleco updated Temu's Refund and Return Policy to clearly distinguish between the 14-day statutory withdrawal right and Temu's voluntary extended return options. This ensures that EU consumers are not misled about which protections stem from EU law and which are offered by Temu voluntarily.

- In relation to the **transparency of trader information**, Whaleco improved the visibility of trader status and contact details. A dedicated "Trader Information" page now provides address, trade register, registration number, email, and telephone number, while product pages label traders more clearly as "Sold by Trader [name]".

- In relation to **consumer contact with Whaleco**, the "Company Info" and "Imprint" sections were renamed and repositioned to make contact details easier to locate, and an additional customer service phone number and email address were added across all EU/EEA versions of Temu, alongside expanded multilingual chatbot support.

- In relation to **consumer reviews and ratings**, Whaleco clarified the calculation of product star ratings and the criteria for "recommended" or "positive" reviews. Additional safeguards were introduced to reduce the risk of misleading review displays, while internal monitoring processes against fake or incentivised reviews were strengthened.

Whaleco recognises the importance of addressing systemic risks proactively, rather than relying solely on mitigation measures once risks have materialised. By redesigning certain aspects of Temu, such as promotional mechanics, review presentation, and consumer information flows, Whaleco has directly reduced the potential for systemic consumer risks to arise. Additional changes to the platform have limited opportunities for traders to engage in misleading practices and enhanced the ability of EU consumers to exercise their statutory rights with clarity and confidence.

Below is a snapshot of Whaleco's risk assessment results.

Sub-Module	Inherent Systemic Risk	Control Strength	Residual Risk
Consumer Protection	Medium-High (4/5)	Somewhat Effective (3/5)	Medium (3/5)

B. Assessment of the Systemic Risks

Pursuant to Article 34(1)(d) of the DSA, Whaleco identifies, analyses, and assesses systemic risks related to economic harm, mental well-being, and lack of transparency that may stem from Temu's design, functionalities, or third-party use, in particular by traders. While Whaleco conducted risk assessments for all Temu attributes and influencing factors mapped in **Section IV**, the following focuses on factors assessed to have a substantial impact on consumer protection risks.

Based on consumer journey simulations, Whaleco categorises risks related to consumer protection into three main thematics:

- **Potential economic harm to consumers,** assessing risks of financial loss or distorted choices from misleading offers, scams, or other unfair commercial practices.

- **Potential impact on users' mental well-being**, considering whether Temu's design or features could foster compulsive use, addictive shopping, or other negative psychological effects.

- **Potential lack of transparency**, concerning whether users receive clear and accessible information about their rights and how the platform functions.

The following paragraphs discuss, in the hypothetical absence of Whaleco's existing mitigation controls, how Temu's core characteristics, other services and features, and the influencing factors in Article 34(2) of the DSA could give rise to systemic consumer protection risks.

Unlike the Product Compliance, IP, and Content Compliance modules, where risks arise primarily from product listings or user-generated content, consumer protection risks may result directly from Temu's own designs, features, or services. For these systemic risks, Whaleco's approach has been to enhance or, in some cases, remove relevant designs to reduce inherent systemic risks. Accordingly, these

efforts are discussed in this section rather than under mitigation measures, as they directly lower inherent systemic risks.

i. Core Characteristics

Each of Temu's core characteristics, i.e., (1) hosting traders, (2) hosting product listings, (3) accommodating EU users, and (4) facilitating online marketplace sales, can give rise to certain systemic consumer protection risks relating to the three thematics or influence the probability or severity of the risks.

Risks of economic harm: fake or duplicate trader accounts. Rogue traders may attempt to evade onboarding controls with fake or duplicate accounts, using stolen identities, thereby increasing the risk of fraudulent activity. Whaleco mitigates this risk by preventing duplicate trader registrations through comprehensive verification process, which rejects applications submitted with previously used identity details.

Risks of economic harm: false, incomplete, or misleading product descriptions. Traders' product listings may contain false or incomplete textual or visual product descriptions that may mislead consumers, such as false discounts, urgency or scarcity tactics, false health or green claims, or fake or digitally altered images that misrepresent a product's size, quality, or functionality, resulting in uninformed or inaccurate purchasing decisions.

During the Relevant Period, Whaleco introduced platform changes to inherently reduce these risks, including:

- **Enhanced display of RRPs.** Any RRP indication is now clearly labelled with the abbreviation "RRP" and a clear explanatory note through the "(?)" icon. Consumers can now easily access explanations of RRP in multiple places, including by hovering over the "RRP" text, figure, "(?)" icon, or the "What's RRP" message on product detail pages.

- **Introduction of the display of the lowest recent price ("LRP").** Product pages now display the lowest price at which the product was offered in the last 30 days, ensuring that consumers can easily verify the basis of a discount.

- **Clarified stock indicators.** Where a product listing displays an "almost sold out" or similar label, a "(?)" icon now provides the following disclaimer: "Sellers are responsible for managing their inventory numbers and decide whether to display the label. A product with this inventory label may be restocked later by the seller".

Transparency risks: traceability of traders. Lack of visibility of trader identity impedes consumers from understanding their transactional counterparty or exercising their statutory rights. During the Relevant Period, Whaleco enhanced transparency by adding a dedicated "Trader Information" link to each product page, which leads to a comprehensive trader information page.

Transparency risks: scale, linguistic and geographic complexity. The large scale and linguistic diversity of both product listings and the EU user increase the risk that mandatory disclosures and consumer information may be missing, mistranslated, or incorrectly localised. This not only affects special product categories requiring additional disclosures, such as safety warnings and health disclaimers, but also extends to general information on terms, taxes, and product characteristics. Such gaps may mislead consumers and breach statutory requirements, a risk heightened by the large number of traders unfamiliar with EU rules and the geographic diversity of EU users, which complicates consistent oversight.

Transparency risks: lack of awareness of statutory rights. Consumers may be misled if they are not clearly informed whether they are purchasing from a trader or a non-trader, or if platform operator details are difficult to access.

During the Relevant Period, Whaleco addressed transparency risks regarding Temu and contact details by:

- Renaming the "**Company info**" section as "**Get to know us**".
- Renaming the "**Imprint**" section as "**Company Details – Imprint**" and moving it higher in the navigation hierarchy, directly under "Contact us", to make it more intuitive.
- Adding a **customer service phone number, together with an additional customer service email address** dedicated to general issues (beyond the two addresses already provided for legal and privacy concerns).
- Consolidating all contact options, such as telephone, emails, and chatbot, under the "Contact us" section for greater clarity.

Transparency risks: clarity of responsibilities. Consumers may be misled about which entity is responsible for shipping, delivery, after-sales support, or refunds. In this context, Whaleco significantly lowered this inherent systemic risk by updating Temu's Terms of Use to expressly clarify responsibilities, including that:

- Consumers may submit withdrawal declarations directly to traders or via Temu, who will automatically forward them for processing; if opting to do so via Temu, consumers may, for example, use the Return/Refund button in the "Your Orders" page.
- Temu provides traders with customer service tools but may also assist consumers directly by facilitating communication or identifying relevant complaint information.
- While Temu assists with customer services and withdrawal processing, the sales contract remains strictly between the consumer and the trader.
- Consumers are also informed that, where applicable, they may act as importers of products, and Temu may appoint a freight forwarder to handle customs duties, taxes, and fees on their behalf.

ii. Services and features

Besides Temu's core characteristics, the other services and features offered on Temu to facilitate and promote sales between traders and consumers may also influence consumer protection risks. A detailed description of these features is available in **Section IV** of this Report. Whaleco discusses the services and features that are defined as influencing factors under Article 34(2) of the DSA in the next section.

a. Product reviews

Risk of economic harm: manipulated or inauthentic reviews. Reviews play a central role in consumer choice and may be manipulated by traders through incentives. In the absence of effective moderation mechanisms, consumers may not be able to clearly distinguish between authentic and inauthentic feedback. Nonetheless, Temu's review process ensures integrity by allowing only consumers who purchased relevant products to submit reviews, creating a direct link between the

reviewer and the product. Furthermore, Temu's recommender systems prioritise reviews with clear, relevant, and high-quality content, thereby limiting the visibility of manipulated or inauthentic reviews that are often irrelevant or unclear to EU users.

Transparency risks: lack of transparency of review recommendations. Temu uses algorithmic models to determine which reviews are displayed more prominently. [Confidential]

Throughout the Relevant Period, Temu reduced transparency risks by:

Clarifying default rankings. Reviews are now clearly labelled as displayed in "Recommended" order, with a link explaining its meaning. Consumers can change the display order through available sorting options, including "Most recent", "Highest rating", and "Lowest rating". A toggle or the "See all reviews" link allows users to easily select their preferred view, giving them control over how reviews are presented.

- **Disclosing star rating methodology**. Star ratings are calculated as the average of verified consumer ratings, as disclosed in the Review Guidelines.

- **Removing potentially misleading labels.** Statements such as "[XX]% positive reviews" and "Recently, [XX] people gave this a 5-star review" were discontinued in July 2024.

b. Limited chat function

Risk of economic harm: manipulative or fraudulent chats. Temu offers limited chat functions that allow consumers to interact with traders. Traders could misuse chat functions to pressure or mislead consumers. Whaleco mitigates this by restricting chats to specific order contexts; traders cannot proactively contact users, and no trader-to-trader or consumer-to-consumer chats are allowed.

Impact on mental well-being: inappropriate chats. Risks of traders potentially using the limited chat forum to discuss inappropriate content that impacts consumers' well-being, such as harassment, stalking, gender-based violence, and bullying, are reduced by the restrictive chat design and by policies prohibiting illegal or harmful content, including the Terms of Use, Community Guidelines, and Review Guidelines, as discussed in the Content Compliance sub-module in **Section VI**.

c. Logistics and payments

Risk of economic harm: late or undisclosed delivery charges. Consumers may perceive certain charges (e.g., import duties, cash-on-delivery ("**COD**") fees) as only emerging late in the order process. Whaleco mitigates this by displaying a full price breakdown (product price, VAT, delivery fees, and estimated import duties) on the checkout page before payment is confirmed. COD fees or any surcharges are disclosed upfront, before the consumer completes payment, preventing unexpected costs at delivery. Finally, Whaleco has ensured that the information disclosed to consumers is adhered to by traders by imposing relevant contractual obligations.

Risk of economic harm: payment fraud or scams. Potential risks arise when traders attempt to misuse Temu to commit fraud or scam consumers. To address this risk, Whaleco has implemented a structured checkout flow, including requirements for electronic payments. In line with EU consumer law, the order confirmation button now explicitly states "Order and Pay", making it clear to consumers that placing the order creates a binding payment obligation.

In addition to the above, Whaleco has implemented changes in its contractual framework, explicitly prohibiting traders from soliciting or accepting payments outside of Temu (*c.f.* §8.5 of Terms of Use), limiting consumer exposure to scams such as fake transfers or diversion to unverified channels. At the

same time, Whaleco has implemented contractual safeguards through the Seller EU Services Agreement, requiring traders to comply with Temu pricing rules and ensuring that consumers are charged only the amounts disclosed during checkout. Finally, sales contracts between traders and consumers are standardised.

Transparency risks: awareness of minimum order value. To reduce the risk of the minimum order value being insufficiently displayed on Temu during the Relevant Period, Temu introduced a top banner on the landing page showing the applicable minimum order value, ensuring visibility of this information at the start of the shopping experience. The minimum order value is also explicitly provided at §10.1 of Temu's Terms of Use. The minimum order value is now displayed in the shopping cart. If the order value is below the minimum threshold, the call-to-action button at checkout indicates this, and users cannot proceed to payment until the minimum order value is reached.

Transparency risks: estimated delivery time. Consumers may at times find delivery timelines unclear or inconsistent. The risk of unclear disclosure of delivery times specifically is more pronounced due to delivery dates being described as "approximative" (*c.f.* Temu's Terms of Use, §10.6). To reduce the risk, during the Relevant Period, Whaleco enhanced transparency by displaying the estimated delivery date for orders. In addition, consumers are covered by Temu's Late Delivery Compensation Policy, which provides compensation in cases where deliveries are delayed beyond the indicated timeframe.

d. Customer services

Risk of economic harm: irremediability. In accordance with EU consumer law, Temu provides EU users with all the required remedial options, such as order cancellation, refunds, and returns, in a manner that reduces the risk of economic harm. To that end, Temu provides additional assurances through the Purchase Protection Program, which guarantees full refunds for mismatched, damaged, undelivered, late, or lost products. To mitigate the inherent systemic risk of uncertainty regarding available escalation and mediation pathways if traders fail to fulfil their contractual obligations vis-à-vis after-sales services, Temu has created a dedicated page explaining the Purchase Protection Program and sets out the process in a Q&A style section in the Platform's Support Center.

Temu offers promotions that are subject to conditions - for example, credits that are revoked when an order is cancelled. While such conditions relate only to promotional benefits, there is a risk that consumers may interpret them as restrictions on statutory withdrawal or refund rights. Similarly, exceptions to returns (e.g., for hygiene reasons or customised products) must be carefully distinguished to avoid confusion. To mitigate this inherent systemic risk, Temu ensures that promotional restrictions do not override statutory protections by updating its Return & Refund Policy in all EU/EEA languages to clarify that promotional terms do not exclude statutory rights. This policy explicitly explains exceptions consistent with Article 16 of the CRD (e.g., sealed health products, customised products), reducing the scope for overbroad "no returns" statements.

Temu also provides consumers with an escalation mechanism in the event of unresolved cases, which are escalated from a chatbot to a live agent, followed by escalation to a specialist team (e.g., Trust & Safety or Customer Service team). To further reduce the potential economic harm to consumers and expedite the resolution of after-sales issues, during the Relevant Period, Temu has expanded the contact channels available to its users by introducing hotline customer service in the EEA with human operators, supplemented in some languages by voice bots.

Transparency risks: accessibility of remedial information and options. A common design risk in online marketplaces is return, cancellation, or refund tool functions not being readily displayed and visible to consumers. During the Relevant Period, Temu has adjusted its User Interface design and support flows to make remedial options easier to access:

- **"Return & Refund" button.** A dedicated button is now available via the "Contact Us" page and consumer accounts, reducing navigation barriers.

- **CRD withdrawal form in all EU/EEA official languages.** Temu facilitates the exercise of statutory withdrawal rights by providing the CRD withdrawal form in all EU/EEA official languages, in line with CRD Article 6(1)(h) and Annex I(B). Consumers are also informed that statutory remedies apply even after the 90-day return window, now explained in the Return & Refund Policy.

Transparency risks: unclear or insufficiently localised customer service processes. The provision of after-sales customer support may give rise to the risk of unclear or insufficiently localised customer service processes. There is a risk that response times, complaint handling procedures, and escalation mechanisms are not clearly disclosed or defined, hindering consumers' understanding of available redress. In addition, if customer service teams are not sufficiently localised (e.g., lack of EU language coverage, or delays due to time-zone misalignment), consumers may face barriers or delays in resolving disputes. To address these inherent systemic risks arising from after-sales customer services, Whaleco has designed Temu's after-sales services to be accessible, multilingual, and compliant with EU consumer protection standards. Temu offers clear contact channels, allowing consumers to reach customer service via multiple entry points on the website and app (e.g., "Contact Us", "Support", "Messages", and the DSA Help Page). In addition to these contact channels, a dedicated single point of contact under Article 12 of the DSA (DSA-point-of-contact-users@eur.temu.com) is published and accessible from the DSA page and app settings. Consumers can submit inquiries through these contact channels in their local EU language and receive responses in the same language, reducing risks of exclusion. [Confidential]

e. Promotional activities

Whaleco assesses below consumer protection risks from promotional activities both on and off Temu, including its sales events and A&I Programme. Temu's recommender systems, which are also part of the on-platform interactive activities, are addressed in the section as a DSA Article 34(2) influencing factor. [Confidential]

Transparency risks: rules of interactive activities. A higher quantity of promotions can create transparency risks, as consumers may find it more difficult to clearly understand, compare, and track the applicable terms and conditions of each offer. The transparency risk related to disclosing the exact terms and details of the interactive activities is low on Temu because, throughout their participation in a programme, relevant information is easily accessible to users. At the start of the programme, a disclaimer in the form of a text field informs users about key aspects of the programme (steps, benefits, minimum order value to receive the benefit, and the validity period). This can also be retrieved on demand through an easily accessible "Rules" button that is clearly displayed. [Confidential]

iii. DSA 34(2) influencing factors

Whaleco has further evaluated the specific influencing factors outlined in Article 34(2) of the DSA and their potential impact on the systemic risks in relation to consumer protection. Detailed descriptions of these influencing factors are available in **Section IV** of this Report.

Whaleco has considered the influence of intentional manipulation of its service, especially by traders in relation to trader accounts, product descriptions, payment and by traders and consumers in relation to product reviews. Where relevant, Whaleco has also considered the specific regional or linguistic diversity of the consumer population, in particular in relation to transparency risks regarding consumers' statutory rights. The amplification and potentially rapid and wide dissemination of illegal

content and information is primarily addressed in the Product Compliance, IP, and Content Compliance module.

a. Recommender systems

Risk of economic harm: Recommender systems are applied on Temu in three contexts: product listings, product reviews, and promotions. In accordance with Article 34(2)(a) of the DSA, Whaleco's risk assessment also considers how the design of recommender systems and other algorithmic systems shapes systemic risks associated with the operation of a VLOP, including risks in relation to consumer protection.

Whaleco minimises the consumer risks by providing users with a "Personalised recommendation" toggle, allowing them to disable personalised recommendations (e.g., recommending products and promotions based on browsing, searching, and purchasing history). When the toggle is deactivated, recommendations will be based only on other non-personalised factors, ensuring user autonomy. In addition, Whaleco has designed Temu to allow users to adjust how product reviews are displayed, such as ordering them from highest to lowest rating (or vice versa), or by most recent.

Risks to mental well-being: addiction due to infinite scrolling. Contrary to social media platforms, Whaleco considers the risk of addiction to be modest on Temu because, even though its main page contains an infinite scrolling of product recommendations, those are inherently unlikely to entertain as such and offer no opportunity to interact with other users, because scrolling on Temu serves a transactional purpose with lower emotional variability. [Confidential]

Transparency risks: recommender systems disclosures. Whaleco has effectively reduced transparency risks by setting out, in plain and intelligible language, the main parameters used in its on-platform recommender systems in accordance with Article 27(1) and (2) of the DSA. The DSA Help Page includes information about the relative importance of the main parameters used in the recommender system, allowing recipients of Temu's services to clearly understand why certain content is recommended to them and how Temu prioritises content displayed to and viewed by consumers. The information is presented in short, simple sentences, and the main parameters are listed in bullet-point form to aid comprehension. [Confidential]

b. Content moderation systems

Transparency risks: false negatives and positives of review moderation: As detailed in the Product Compliance, IP, and Content Compliance module, Temu's content moderation systems, which integrated automated detection and human review, are the cornerstone to mitigation consumers' exposure to the dissemination of illegal content. In addition to risks in relation to illegal content, content moderation systems themselves may give rise to specific consumer protection risks, including the risk of disproportionate or ineffective automated moderation. Temu's automated detection system screens reviews before and after publication. However, such automated tools may produce both false negatives (e.g., allowing misleading claims) and false positives (e.g., removal of legitimate consumer reviews). Both under- and over-enforcement undermine consumer protection and compliance with the DSA, particularly where consumers are not clearly informed of moderation outcomes or avenues for redress.

c. Applicable terms and conditions and their enforcement

Transparency risks: lack of transparency of Temu's terms and conditions. In accordance with Article 34(2)(c) of the DSA, Whaleco's risk assessment considers how contractual terms and policies governing activity on Temu shape systemic risks associated with the operation of a VLOP. Temu's

consumer experience is shaped by a broader set of contractual and policy documents (e.g., Privacy Policy, Community Guidelines, etc.) which define consumer rights and obligations, govern after-sales processes, regulate content creation and behaviour, and set rules on data processing and personalisation. While these documents collectively aim to provide transparency and safeguards, their complexity and interaction create potential risks for consumers, namely:

- **Mandatory consumer rights in contractual terms.** If key statutory rights (withdrawal, refunds, remedies) are not presented across different contractual and policy documents, consumers may be uncertain about their rights and who is responsible for fulfilling them. To address this risk, Whaleco has taken steps to ensure that consumer rights are explained clearly and consistently across its contractual and policy framework (Terms of Use, Return & Refund Policy, DSA Help Page, Seller EU Services Agreement).

- **Prominent display of Terms of Use and incorporated policies**. Consumers may be misled or deprived of their rights if the Terms of Use and related documents (Privacy Policy, Community Guidelines, Review Guidelines) are not prominently or clearly displayed. Whaleco has improved visibility and accessibility of contractual documents and mandatory disclosures by: a) ensuring that age restrictions (18+) and minimum order values are displayed prominently on entry (via banners) and during checkout; b) hyperlinking core policies (Privacy Policy, Community Guidelines, Review Guidelines) in the Terms of Use and making them accessible at the bottom of every webpage and app screen; c) prominent display of the Return & Refund Policy at the homepage and at checkout; d) integrating key consumer rights in the Return & Refund Policy to reduce fragmentation across multiple linked documents; and e) launching the Transparency Centre as a central hub containing Temu's policies, reports (e.g. transparency, audit, systemic risk), tools and APIs, thereby giving users and regulators one place to see how Temu works behind the scenes.

- **Transparency of liability limitations and indemnity.** Temu's Terms of Use contain liability caps, exclusions, and indemnities, which, albeit valid, carry an inherent systemic risk that consumers may misunderstand them as potentially overriding their mandatory statutory rights (e.g., conformity guarantees, product liability). To prevent this risk from materialising, Temu clearly states that limitations of liability do not affect mandatory statutory rights under EU law (e.g., conformity guarantees, product liability) and provides simple explanations in FAQs and help pages, clarifying that liability caps do not override consumer protections. In addition, in line with Article 14 of the DSA, Whaleco ensures that its Terms of Use are drafted in a clear, plain, intelligible, user-friendly and unambiguous manner.

- **Communication of dispute resolution pathways.** If complaint-handling and mediation channels are not prominently displayed, consumers may not clearly perceive the redress options available to them. To reduce this risk, Whaleco has made its complaint and redress mechanisms more visible by including reference to available redress routes, including Temu's mediation and appeal process, in the DSA Help Page. Temu's DSA Help Page sets out the timeframe and conditions for submitting an appeal, explains the grounds on which an appeal may be successful and a decision reversed, and identifies the circumstances in which users are entitled to contact an out-of-court dispute settlement body for dispute resolution purposes. To further mitigate any risks arising from insufficient communication of available dispute resolution pathways, Temu facilitates customer service escalation, whereby consumers are directed towards Temu's Customer Service team for assistance with disputes, including mediation with traders.

- **Disclosure of promotional restrictions in Temu's policies.** Consumers may be misled if promotional terms are hidden or insufficiently prominent in Temu's Terms of Use or related

policies. Residual risk arises, for instance, if clauses are not accompanied by an explanation that statutory withdrawal rights still apply. To reduce this risk, Temu's Return & Refund Policy now clarifies that statutory withdrawal rights apply regardless of promotional wording.

- **Clarity on sanctions and consequences of breach of contractual arrangements.** Temu's Terms of Use list prohibitions and threatened penalties (removal of content, cancellation of purchases, suspension of accounts) in the event of a breach of the Terms of Use. Absent a clear explanation of what happens to pending orders, refunds, or rewards in such cases, consumers may be uncertain about the financial effects of enforcement measures. To reduce this inherent systemic risk, Temu specifies threatened penalties in the Terms of Use.

d. Systems for selecting and presenting advertisements

Article 34(2)(d) DSA requires Whaleco to assess how the systems for selecting and presenting advertisements can influence and mitigate systemic risks with regard to consumer protection. However, during the Relevant Period, and as of the date of the submission of this report, Temu did not offer advertising services on Temu to traders or other sponsors. Such systemic risks thus did not arise.

e. Data-related practices

Data-related practices. In line with Article 34(2)(e) DSA, Whaleco's risk assessment considers how data-related practices may contribute to consumer protection risks, such as the risk of insufficient transparency about data use affecting consumer decision-making. If Temu's Privacy Policy fails to clearly explain how consumer data is processed, consumers may be misled about the scope of data use or wrongly assume such practices do not occur. While GDPR governs the lawfulness of processing, a lack of policy clarity or opaque design choices may also constitute misleading omissions under consumer law. Assessment of data-related practices will be detailed in the Fundamental Rights module.

iv. Inherent systemic risk evaluation

Sub-module	Inherent Systemic Risk Score	Assessment Findings
Consumer Protection	**Medium-High**	**Probability (High - 5/5):** For consumer protection, the evidence confirms daily occurrences of consumer protection risks on Temu with regards to attempts of scam/fraud or inappropriate interactions by third parties, exposing Temu's consumers to systemic risks of economic harm and mental well-being.
		Severity (Medium - 3/5): The primary scale of harm is psychological harm and economic loss to consumers and rights holders, which is generally considered less severe than physical harm. The harm to consumers is also partially remediable through refunds. Due to the high number of users affected, the severity rating is nevertheless considered high.

C. Mitigation Measures

This section addresses mitigation measures applied by Whaleco in addition to the wide variety of ways in which it has conceived or adjusted the design of Temu in order to reduce the inherent systemic risk

that it generates. In broad terms, where risks to consumers derive directly from the design of Temu, mitigation measures are likely to be found in changes to that design. Such changes are addressed in the previous section because they directly reduce the inherent systemic risk of Temu. In contrast, where the risks to consumers derive from the actions of third parties such as traders or users, Whaleco focuses on measures it can take to mitigate such risks.

The mitigation measures discussed below fall within the six control groups within Whaleco's DSA mitigation framework, including (1) governance, risk & compliance oversight, (2) policies & standards, (3) user management & onboarding compliance, (4) detection & enforcement, (5) user rights & redress mechanisms, and (6) external engagement. Whaleco assesses control strength from these six control domains. Because this module addresses various types of consumer protection risks, mitigation measures for which may cross several different control groups. For efficiency, Whaleco discusses the mitigation measures by risk types rather than by the control groups.

Whaleco assessed the overall strength of the mitigation measures through defined performance metrics and fact-finding questions developed in accordance with the methodology in **Section III**. Based on Whaleco's evaluation, the overall effectiveness of controls with respect to the Consumer Protection module was assessed as **"Somewhat Effective"**.

i. Mitigation measures addressing risks stemming from Temu's Core Characteristics

Temu's operational characteristics, specifically, its role in hosting third-party traders and facilitating cross-border transactions for EU users, create a consistent need for advanced technical and human moderation. Whaleco has implemented targeted measures to mitigate the risks involved, focusing on transparency, trader accountability, product listing integrity, and the clarity of consumer rights and remedies, including enhancements made in collaboration with EU regulators during the Relevant Period.

Risk category	Mitigation measures: Temu's Core Characteristics
Risks of economic harm: fake or duplicate trader accounts	Whaleco has established a comprehensive trader management framework to mitigate the systemic consumer protection risks arising from the number and diversity of traders on Temu and the possibility that they may misuse it. More specifically, Whaleco blocked attempts by traders to create fake or duplicate accounts by cross-verifying their identities against third-party databases, as well as the Trader Blocklist through entity-linkage recognition technology. This is further described in the Illegal Content, Product Compliance and IP module.
Risks of economic harm: false, incomplete, or misleading product descriptions	Whaleco has established a unified content moderation framework that integrates automated detection with human review of product content, including potentially false, incomplete, or misleading product descriptions. The automated moderation system utilises keyword and image recognition to detect potentially fraudulent product descriptions. Whaleco discusses more details about the content moderation framework in the Product Compliance, IP, and Content Compliance in relation to its mitigation measures relating to detection & enforcement.

ii. Mitigation measures addressing risks stemming from Temu's other services and features

Beyond its core marketplace functions, Temu offers additional services and features that influence consumer protection risks, such as reviews, interactive activities, the A&I Programme, payments, and

customer service channels. Whaleco has strengthened these areas to ensure compliance with EU consumer law, improving clarity, accessibility, and safeguards against misleading practices, particularly in response to consumer feedback and engagement with EU regulators.

Risk category	Mitigation measures: Temu's other services and features
Risk of economic harm: Manipulated or inauthentic reviews	As discussed above, Temu is designed to allow only user accounts that have purchased a product on Temu to submit a review for that product. This design feature alone substantially reduces the inherent systemic risk of manipulated or inauthentic reviews. In addition, Whaleco has implemented a layered moderation framework designed to ensure that only authentic and compliant product reviews are displayed on Temu. [Confidential] • **Pre-posting moderation.** All product reviews submitted by users on Temu are made publicly available only after having undergone automated screening, resulting in approval, rejection or escalation to manual assessment. If the automated screening system detects prohibited or non-compliant content, such as prohibited terms and phrases, the product review is automatically blocked from publication and remains unpublished while undergoing manual assessment. For complex content such as multilingual text or content embedded in images and videos, Whaleco employs machine translation and algorithms to capture concealed or non-standard violations. Product reviews blocked from publication at this stage are not ranked and scored in the context of the recommender system. • **After-posting moderation.** Consumers may report reviews they suspect to be false, misleading, or otherwise non-compliant by using the "Report" function available on every review. Product reviews that are reported by users are manually assessed by Whaleco's Trust & Safety team (TST), which evaluates each review and takes appropriate action, including removal where the content violates Community Guidelines. Once removed in response to a user report, a review is excluded from the "Recommended" reviews on Temu. [Confidential] • **Policy framework**. The Community Guidelines and Review Guidelines expressly prohibit incentivisation, fabricated endorsements, and irrelevant or abusive content. These rules are communicated to users at the time of posting .
Risk of economic harm: manipulative or fraudulent chats	Temu does not enable communications between users, Temu does not allow traders to contact a user other than in relation to a specific order that user has placed or following a product related enquiry. This technical design prevents an inherent systemic risk that might otherwise have arisen. Whaleco also enforces policies and technical safeguards aimed at preventing consumer manipulation or fraud through chat interactions. Terms of Use prohibit traders or agents from arranging for the sale of listed items or the payment of fees outside the context of Temu. Trader chat is monitored for diversion attempts and abusive conduct, and users can also directly report suspicious chat behaviour, triggering manual review and intervention by customer service and compliance teams.

Risk category	Mitigation measures: Temu's other services and features
	Penalties (including account suspension) apply to traders who breach the rules. Moreover, various blacklisted terms trigger blocking messages that prevent non-compliant communication. Of note, consumers remain protected by the Return & Refund Policy (e.g., free first return within 90 days) and the Purchase Protection Program, which ensure full refunds in cases of defective or undelivered products.
Risk of economic harm: payment fraud/scam	As described in the section on Systemic Risk assessment, Whaleco has implemented contractual prohibitions and structured processes that reduce opportunities for fraudulent or misleading payment practices, as well as standardising the checkout process and strengthening contractual and technical safeguards. These designs protect consumers by directly reducing the opportunities to misuse Temu's systems to defraud consumers and enhancing consumers' understanding of their purchasing decisions. In addition, Whaleco implements a variety of measures intended to mitigate the risk of potential fraud enabled by, in particular, inadequate authentication of the user attempting to purchase products on Temu. Temu applies Payment Card Industry Data Security Standard (PCI-DSS) requirements when processing card information, providing a recognised level of protection for consumers' payment data. Moreover, Purchases on Temu can be completed using electronic payment methods (e.g., credit/debit card, PayPal, Klarna). Credit/debit cards need to be verified. Third-party payment service providers (e.g., Klarna, PayPal) apply their own authentication requirements, including two-factor verification and account validation, which provide additional safeguards reducing the exposure of consumers to unauthorised transactions. Temu relies on contractual requirements and third-party safeguards to ensure consumers are not misled about "Buy now, pay later" (BNPL) promotions. Temu prohibits misleading promotional language by traders or affiliates suggesting that BNPL is "free" or "risk-free" without conditions. Promotional references to BNPL must comply with Temu rules and EU consumer law. Moreover, the licensed third-party payment service providers offering BNPL services are subject to EU consumer credit and transparency rules requiring them to present interest rates, repayment conditions, and potential fees clearly to consumers before they confirm a BNPL purchase.
Risk of economic harm: A&I Programme	Whaleco has implemented a range of mitigation measures to reduce the risk to consumers which could arise from Temu's A&I Programme. [Confidential] • **Temu Affiliate Policy and Temu Influencer Policy**. Affiliates and Influencers must adhere to Temu's A&I Programme Policies which, in turn, require them to comply with EU consumer protection law. Any Affiliate or Influencer found to have engaged in any fraudulent, criminal, or dishonest activity in connection with the A&I Programme is disqualified from the Programme and may not earn further commissions. [Confidential]
Risks of economic	Whaleco's efforts to mitigate risks of economic harm in relation to potentially misleading interactive activities include three parts:

Risk category	Mitigation measures: Temu's other services and features
harm: misleading interactive activities	compliance guidelines circulated by the LCT, LCT compliance review of proposals and issuance of advice, and an annual retrospective sample inspection. [Confidential]
Risks to mental well-being: interactive activities stimulating addictive behaviour	Whaleco's efforts to minimise risks to the mental well-being of consumers from Temu's interactive activities focus on the design of Temu itself. [Confidential] In addition to limiting the types of interactive activities available, and the extent to which users can participate in them, Temu applies a further set of measures to mitigate the risks to mental well-being. [Confidential] • **Customer support and remedial options.** A customer support team is available for users to exercise their statutory risks regarding any orders placed - either in the context of an interactive activity or otherwise. Whaleco also offers a generous refund policy which protects users in the unlikely event that a promotion is considered to be misleading by users and/or external stakeholders. Consumers may cancel orders at any time before shipment. Temu fulfils its obligations regarding the statutory right of withdrawal under the Consumer Rights Directive and, without prejudice to those rights, voluntarily offers a 90-day return policy on most purchases, including free shipping for the first return per order. [Confidential]
Risks to mental well-being: A&I Programme	Only products that have already been screened and successfully listed on Temu are eligible for promotion in the A&I Programme. Products that are not listed on Temu are not eligible for promotion through the A&I Programme. [Confidential]
Impact on mental well-being: inappropriate chats	Temu provides only very limited chat functions, essentially restricted to communications between traders and users in relation to specific orders that have been placed. This technical design very substantially avoids the inherent systemic risk that might otherwise have arisen. Temu mitigates this very limited risk by additional measures: • **Contractual safeguards.** The Terms of Use and Community Guidelines prohibit unlawful, abusive, or manipulative communications. Merchants are prohibited from diverting consumers off-platform, using offensive language, or misusing chats for unrelated solicitations. Violations can result in financial penalties or account suspension. • **Monitoring and security.** Chats are subject to risk-control filters (e.g., blocking pornographic or politically sensitive content, diversion attempts) and business controls (e.g., restricting traders from encouraging order cancellations due to stock-outs) .

iii. Mitigation measures tailored to Article 34(2) influencing factors

In line with Article 34(2) of the DSA, Whaleco has taken steps to mitigate risks linked to recommender systems and content moderation. This includes increasing transparency around how recommender systems rank or prioritise information, prohibiting misleading or manipulative trader practices through

contractual standards, and combining automated screening with human oversight to ensure proportionate and effective enforcement supported by clear redress mechanisms.

Risk category	Mitigation measures tailored to Article 34(2) influencing factors
Risks of economic harm: recommender systems	Whaleco takes proactive steps to mitigate any risks to consumers arising from the design and implementation of Temu's recommender systems. These should be considered in conjunction with the design aspects of those systems, for example, the options provided to decline personalised recommendations altogether. Temu's content moderation framework excludes non-compliant or IP-infringing products from recommendations, only including items that have passed pre-listing screening. When non-compliant products are later detected through continuous screening or external feedback, they are immediately removed from all recommendation feeds and can only be reinstated after full compliance clearance. [Confidential]
Transparency risks: false negatives and positives of review moderation	Whaleco enhances the effectiveness of its content moderation by various measures designed to induce traders to conduct their activities in a manner that does not mislead consumers or otherwise undermine their ability to take undistorted transactional decisions: The Terms of Use, Community Guidelines, and Review Guidelines set out clear contractual prohibitions on misleading advertising or urgency claims, manipulative reviews and similar content. The Seller EU Services Agreement incorporates obligations on traders to comply with these standards, and authorises sanctions where violations occur. Breaches can lead to suspension, delisting, or termination, ensuring that moderation actions are backed by enforceable contractual provisions. To mitigate the inherent systemic risk of disproportionate or ineffective automated moderation, Temu combines automated detection with human review and accessible redress. Automated filters detect potentially unlawful or misleading content, with inconclusive cases escalated to human moderators. Those moderators undergo onboarding and continuous training to reduce both over-enforcement (false positives) and under-enforcement (false negatives).

D. Residual Risks and Future Mitigation Measures

Based on Whaleco's enhancements to the design and features of Temu and the additional mitigation measures Whaleco has put in place there to address the systemic risks above, Whaleco assesses the residual risk as **"Medium"**. The following table summarises Whaleco's risk rating results for the Consumer Protection module.

Sub-Module	Inherent Systemic Risk	Control Strength	Residual Risk
Consumer Protection	Medium-High (4/5)	Somewhat Effective (3/5)	Medium (3/5)

To address the residual risks and potential insufficiencies of the existing mitigation measures identified in the Year 2 risk assessment, Whaleco plans on enhancing the mitigation controls against consumer protection risks in the following areas:

Mitigation Type	Description (DSA Article 35)	Controls	Control Enhancement Description
Internal Risk Management & Oversight	Reinforcing the internal processes, resources, testing, documentation, or supervision of any of their activities in ds regards detection of systemic risk	Interactive Activities	**Compliance training**: Whaleco will strengthen its compliance controls for new initiatives of interactive activities on Temu by conducting periodic training for existing and new employees responsible for designing and implementing these interactive activities. The training sessions will cultivate compliance awareness among business teams and reinforce Whaleco's compliance commitments. Training protocols will be broadened, building on the existing framework and evolving based on relevant regulatory developments.
Internal Risk Management & Oversight	Taking awareness-raising measures and adapting their online interface in order to give recipients of services more information	Recommender Systems	**Recommender Systems Disclosures**: Whaleco will enhance the transparency of Temu's recommender systems and relevant algorithmic systems by updating its publicly displayed disclosures to include clear and accessible descriptions of the different types of recommender systems, the main parameters used in each system and the reasons for their relative importance, and options for users to modify or influence the recommendation results, including clear display of options to opt out of personalised recommendations.
Internal Risk Management & Oversight	Taking awareness-raising measures and adapting their online interface in order to give recipients of services more information	Transparency Center	**Transparency Center**: Temu will continue to enhance and expand its disclosures in the Transparency Center, which will serve as Temu's centralised information hub for Temu users to easily access information regarding terms of service, promotional activity rules, consumer rights, and other mandated disclosures. This control enhancement is designed to foster informed consumer decision-making, demonstrate accountability, and ensure readily available access to the information governing the use of Temu's services.
Detection & Enforcement	Adapting content moderation processes, including the speed and quality of processing	Product Descriptions	**Product descriptions with false urgency or scarcity claims**: To further mitigate risks associated with potentially misleading urgency or scarcity claims in product descriptions,

Mitigation Type	Description (DSA Article 35)	Controls	Control Enhancement Description
	notices related to specific types of illegal content and, where appropriate, the expeditious removal of, or the disabling of access to, the content notified, in particular in respect of illegal hate speech or cyber violence, as well as adapting any relevant decision-making processes and dedicated resources for content moderation		Whaleco will implement technical controls restricting the use of specific high-risk keywords by traders within product listings and descriptions. This enhancement will involve the creation and maintenance of a prohibited and monitored keyword list, encompassing terms that may create a false sense of urgency or deceive consumers. This control directly supports compliance with EU consumer protection law by preventing misleading actions and omissions at the point of listing, thereby ensuring that listings are accurate and verifiable.
External Engagement	Reinforcing the internal processes, resources, testing, documentation, or supervision of any of their activities in particular as regards detection of systemic risk	EU engagement	**EU engagement:** Temu will continue to maintain ongoing engagement with relevant European Union institutions, regulatory bodies, and industry stakeholders on matters pertaining to consumer protection law and policy. This proactive engagement will include consultations and structured on-going dialogue aimed at understanding evolving regulatory expectations. This commitment ensures Temu's compliance strategies are aligned with the dynamic EU regulatory landscape, thereby supporting consistent regulatory compliance and promoting fair practices.

VIII. Protection of Minors

Whaleco recognises that minors are vulnerable consumers who merit special protection. While Whaleco conducts risk assessments for all the Temu attributes and influencing factors mapped in **Section IV** in this module, not all factors would have a substantial impact on the risks related to the protection of minors. This module examines the potential systemic risks arising from Temu's functionalities that may have negative impacts on the rights of the child, as enshrined in Article 24 of the Charter of Fundamental Rights of the EU and the United Nations Convention on the Rights of the Child. It reflects Whaleco's efforts to implement appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors on Temu, in accordance with Article 28 of the DSA. For these purposes, Whaleco has focused in particular on the Commission's Guidelines on measures to ensure a high level of privacy, safety and security for minors online, adopted in July 2025, as well as the European Strategy for a better internet for kids (BIK+).

In line with Recital 81 of the DSA, the module covers risks related to CSAM, the exploitation of minors' vulnerabilities, and exposure to harmful, age-inappropriate, or manipulative commercial content and practices.

Many of the risks identified in other modules already apply to underage users. Specifically, the risks described in the Product Compliance, IP, Content Compliance, and Consumer Protection modules are relevant to minors who access the Temu in the EU. Accordingly, risks are only revisited here where there is a dimension that particularly affects the welfare of minors accessing Temu, and sets out additional, tailored risk mitigation measures that address the particular vulnerabilities of minors as EU users.

A. 2025 Highlights

Temu's minor protection risk profile is driven by the fundamental position that Temu is not intended for use by anyone under the age of 18 or defined as a minor by applicable law. Whaleco thus operates a platform intended for adults, while taking measures to address the risks for minors who may nonetheless gain access in accordance with the European Commission's Guidelines on measures to ensure a high level of privacy, safety and security for minors online, adopted in July 2025. The commercial growth of Temu, which has involved a greater number and diversity of users across the EU and a greater number of traders, nonetheless affects the overall scale of risks for minors.

Whaleco has put in place specific measures to address these minor protection risks, demonstrating its adaptive compliance framework. In particular, Whaleco applies an age-gate for adult-only products, which requires the user to confirm that they are over 18 before seeing and accessing the product listing, and a variety of warning labels for other age-inappropriate products, while applying content moderation aimed specifically at identifying CSAM and other exploitative material on Temu. In addition, Temu provides an easy-to-use online reporting form enabling parents and guardians to request deletion of any Temu account that their child has managed to open.

Whaleco's overall assessment is that the inherent systemic risk to minors on Temu is Medium-High and that, after the implementation of mitigation measures, the residual risk is Medium. Whaleco continues to look for ways to reduce those risks further and is eager to engage with external stakeholders in this respect. In particular, Whaleco will be closely monitoring the development of the age verification solutions being rolled out by the European Commission.

Below is a snapshot of Whaleco's risk assessment results.

Module	Inherent Systemic Risk	Control Strength	Residual Risk
Minor Protection	Medium-High (4/5)	Somewhat Effective (3/5)	Medium (3/5)

B. Assessment of the Systemic Risks

Whaleco has carried out its assessment with the assistance of the "5C" typology of risks advocated by the OECD in its report "Children in the Digital Environment: Revised Typology of Risks" and adopted by the European Commission in its Guidelines on measures to ensure a high level of privacy, safety and security for minors online.

Accordingly, Whaleco has considered five categories of risks: namely, Content Risks, Conduct Risks, Contact Risks, Consumer Risks, and certain Cross-Cutting Risks. These categories overlap and interrelate, and in the description below, Whaleco has sought to refer to the most obviously relevant category for any given risk. The categories are summarised in the OECD's table below:

Risks for Children in the Digital Environment				
Risk Categories	**Content Risks**	**Conduct Risks**	**Contact Risks**	**Consumer Risks**
Cross-Cutting Risks*	Privacy Risks (Interpersonal, Institutional & Commercial)			
	Advanced Technology Risks (e.g., AI, IoT, Predictive Analytics, Biometrics)			
	Risks on Health & Wellbeing			
Risk Manifestations	Hateful Content	Hateful Behaviour	Hateful Encounters	Marketing Risks
	Harmful Content	Harmful Behaviour	Harmful Encounters	Commercial Profiling Risks
	Illegal Content	Illegal Behaviour	Illegal Encounters	Financial Risks
	Disinformation	User-Generated Problematic Behaviour	Other Problematic Encounters	Security Risks

* Note: The typology acknowledges risks that cut across all categories ("Cross-Cutting risks"). These risks are considered highly problematic as they may significantly affect children's lives in multiple ways.

Source: OECD and Berkman Klein Centre for Internet and Society at Harvard University.

i. Core characteristics

A core characteristic of Temu that affects whether minors accessing it have a safe online experience is the wide variety of product listings available on Temu.

Conduct risks: **risk of minors acquiring age-inappropriate products.** Under the OECD's 5C framework, this risk is best viewed as a conduct risk, in that it involves the actions of minors on Temu. Traders list a wide variety of products on Temu, including certain products that may be harmful to sell to minors. This includes, e.g., knives and sexual wellness products. If minors can acquire age-

inappropriate products, it may result in physical or psychological harm, such as injuries from knives or distortions in mental development.

Content risks: **risk of exposure to adult-only products**. The exposure of minors to product listings for most age-inappropriate products does not in itself imply a risk that is distinct from the possibility that they may acquire such products. For adult-only products such as sexual wellness products, exposure to the product listing might present a distinct content risk, albeit that this would generally be a lower level of risk than, for example, actual access by minors to pornographic material. [Confidential]

For completeness, Whaleco recognises that traders may seek to use Temu to sell products that are illegal as such. However, the risks associated with such products are not specific to minors accessing Temu but apply regardless of the identity of the user who accesses Temu and purchases the product. They are therefore addressed in the Product Compliance, IP, and Content Compliance module, which describes more generally Whaleco's processes for ensuring that prohibitions on the sale of certain products in its trader policies are enforced.

ii. Services and features

a. Inherent systemic risks relating to Temu's facilitation infrastructure

Content risks: risk of CSAM or exploitative content being disseminated. There is a risk that malicious actors could disseminate CSAM on Temu, for example, by uploading illegal images or text. In practice, this is exceptionally rare. [Confidential] Additionally, the risk of exposure is contained by the fact that, on Temu, users cannot search for CSAM-related keywords, nor can they search for product reviews by users, as such is not an available platform feature.

Contact risks: risk of possible contact between traders and minors. However, the opportunity for contact between traders and minors on Temu is very limited. Traders can initiate contact only after the user has placed an order, and importantly, traders will not know whether the user is a minor because minors, who are not allowed to access Temu, are not identified as such. Whaleco notes that by design, Temu does not enable users to chat or otherwise communicate with each other, and it is not possible for users to reply to product reviews posted by another user. The contact risk for minors arising on other platforms that enable users to communicate with each other thus does not apply to Temu. [Confidential]

iii. DSA 34(2) influencing factors

Whaleco's assessment has taken into account the various factors highlighted in Article 34(2) DSA. Certain factors, such as content moderation systems and the applicable terms and conditions and their enforcement, are significant primarily in the context of mitigation measures, discussed below. Whaleco has considered the influence of intentional manipulation of its service as relevant in the context of the risk of CSAM or exploitative content being disseminated. The amplification and potentially rapid and wide dissemination of illegal content and of information that is incompatible with Temu's terms and conditions is mainly for the risks associated with illegal products that are addressed in the Product Compliance, IP, and Content Compliance module. Two related issues nonetheless arise and are considered in the context of age-inappropriate products in recommender systems, as well as data-related practices related to minors. Risks for minors arising specifically in relation to Article 34(2) factors are assessed below. [Confidential]

a. Data-related practices

Consumer risks: risk of tracking and profiling of minors. Besides a commercial profiling risk, under the OECD's 5C framework, this also represents a cross-cutting privacy risk. If minors access Temu

notwithstanding the Terms of Use, this will lead to their personal data being collected and processed along with the personal data of all users, for example, when creating an account, browsing, and interacting with product listings. This data could then be used to target these users with personalised product or promotional recommendations, although the level of risk is appreciably reduced by the fact that Temu does not collect age-related data.

iv. Inherent systemic risk evaluation

Sub-module	Inherent Systemic Risk Score	Assessment Findings
Protection of Minors	**Medium-High**	**Probability (Medium-High - 4/5):** Internal data indicates a prevalence rate of minor protection-related takedown incidents that is less than [Confidential], 3 other VLOPs operating online marketplaces, more than half, have reported occurrences in their latest Transparency Report, and this risk has been flagged twice by external organisations. This evidence collectively indicates a medium-high probability of occurrence.
		Severity (Medium-High - 4/5): For minor protection, the scope is medium-high as Temu is not intended for minors and there are only [Confidential] minor account deletions, but a conservative approach is taken considering the number of minor persons in the EU. The severity is ranked as high, as minors are a vulnerable group and both CSAM and age-inappropriate products and content may cause severe physical and psychological harm. The harm to minors is also partially remediable through refunds and control mechanisms on Temu relating to minors, resulting in an overall medium high severity rating .

C. Mitigation Measures

Whaleco has reviewed the risk to minors associated with Temu with a view to ensuring that it has in place measures to ensure a high level of privacy, safety and security of minors, as envisaged in the European Commission's Guidelines on measures to ensure a high level of privacy, safety and security for minors online. Whaleco considers these measures appropriate and proportionate in the context of a service that is accessible by minors but not actively targeted at them, but rather intended for adults, reconciling the desire to provide an enjoyable shopping experience for them. In this context, Whaleco has actively considered issues and concerns brought to its attention by external stakeholders.

In the assessment of appropriate and proportionate mitigation measures, Whaleco considers it significant that Temu focuses on offering products for purchase rather than on displaying user-created content. While users can create content in the form of product reviews, this is incidental to the display of specific products for purchase, and those reviews cannot be searched for individually. Whaleco also views it as significant that Temu offers no ability for users to communicate with each other individually, which very substantially avoids the contact risks to minors associated with services that facilitate such communication. Whaleco has moreover taken into account that Temu's nature, purpose and intended use as a marketplace for purchases by means of electronic payment methods by adults reduces the

likelihood of access by minors (at least as compared with, for example, a website offering content intended for minors). [Confidential]

Policies discouraging access by minors. Whaleco makes clear in Temu's Terms of Use, accessible via the homepage, that "*To use the Services, you represent that you are using the Services solely for personal non-commercial) use, and you are at least eighteen (18) years old and the age of majority as defined by applicable laws*". Temu's Terms of Use likewise warn adults to restrict the use of Temu by minors and draw their attention to their own responsibility in this respect. This is reiterated on Temu's Digital Service Act page under the Report a Child Account paragraph, stating that *"The Temu service is not intended for use by anyone under the age of 18 or by minors as defined under applicable laws"*.

Parental deletion of minors' accounts. Accessible and clearly described via the Digital Services Act page on the homepage, Temu provides an easy-to-use online reporting form enabling parents and guardians to request deletion of any Temu account that their child has managed to open. Once a request is verified, the account and all related data will be permanently deleted. During the Relevant Period, Whaleco deleted [Confidential] accounts created by minors in the EU. This feature represents an effective option for parents and guardians, where during the Relevant Period, the average time from notification to deletion of the account was [Confidential]. This period reflects the need for Temu to validate the request in order to ensure that the procedure is not misused against genuinely adult users.

In addition, Whaleco adopts specific measures to mitigate the risks to minors associated with the core characteristics of Temu and its services and features. Based on Whaleco's evaluation, the overall effectiveness of controls with respect to the Protection of Minors module was assessed as "**Somewhat Effective"**.

i. Mitigation measures addressing risks stemming from Temu's core characteristics

Whaleco has adopted targeted safeguards to address risks to minors arising directly from Temu's role as an online marketplace. These include measures to minimise exposure to, or the purchase of, age-inappropriate products, such as age declaration, warning labels, and stricter classification checks, as well as prohibitions on certain product categories. These protections are embedded in product listing and trader management processes and represent the baseline safeguards against risks to minors inherent in Temu's core marketplace functions.

Risk category	Mitigation measures addressing risks stemming from Temu's core characteristics
Content and conduct risks	**Product pre-listing safeguards towards traders.** With respect to unsafe or age-inappropriate products that might be presented to minors on Temu, Whaleco adopts strict controls regarding traders in the pre-listing stage in relation to their product listings. These are described in more detail in the Product Compliance, IP, and Content Compliance module. It should be highlighted that certain age-inappropriate products such as tobacco products and alcoholic beverages are prohibited from sale on Temu, as stated in the Product Safety and Compliance Policy. This policy also goes on to specifically prohibit *"products that encourage or imply drinking under the legal age"*. To ensure enforcement, Temu proactively and reactively takes down non-compliant products with its automated detection and human review and takedown mechanisms. **Warning labels on products for minor protection**. Whaleco applies [Confidential] different warning labels relevant for minors across all its listed products sold on Temu in accordance with both regulatory provisions and stemming from its own initiative. This includes warning

Risk category	Mitigation measures addressing risks stemming from Temu's core characteristics
	labels relating to the EU Toy Safety Directive, labels to differentiate pet toys from children's toys, for sexual wellness toys, the GPSR, pyrotechnic articles, EU cosmetic products regulation, industry practices, and even simply as a Temu response to news reporting, therefore going beyond the required scope of EU regulations. For example, the warning "*Not suitable for children under 36 months. Small parts. Choking hazard.*" stems from the EU Toy Safety Directive, and the warning "*Never leave your child unattended—drowning hazard*" stems from the EU Toy Safety Directive as well as the GPSR. Displayed at the top section of the Product details when viewing a product with a yellow triangular exclamation mark label followed by the word "*Warning*" in bold, these labels clearly communicate that users should pay attention to the minor protection-related information they contain. **Age-gating mechanisms and remediations for adult-only products.** An additional barrier is applied for adult-only sexual wellness product categories. Temu blurs the product listing and if a user searches for this type of product, a pop-up window requires the user to confirm that they are over 18 in order to unblur the images. This measure is particularly relevant in relation to such products in the context of search results. Though Whaleco recognises that minors may intentionally bypass this mechanism by misrepresenting their age, this age-gate, which relies on self-declaration, primarily functions to prevent accidental or unintentional access to such content. A safety-by-design feature of Temu is that all purchases require a means of electronic payment. This further reduces the likelihood that minors will be able to acquire age-inappropriate products, or at least without adult supervision or involvement. Parents or guardians may cancel orders at any time before shipment. Temu fulfils its obligations regarding the statutory right of withdrawal under the Consumer Rights Directive and without prejudice to those rights, voluntarily offers a 90-day return policy for most purchases with free shipping for the first return for each order. These measures make it easier to remedy situations where a minor has managed to discover, order and obtain delivery of an age-inappropriate product. Whaleco also recognises that the effectiveness of its age-gate depends on correctly classifying products as falling within the categories subject to the age-gate. Temu's product categorisation processes involve an initial classification made by the trader and a double-check by Temu, which applies automated detection, followed by human review if a product listing is flagged. Store-specific checks also take place. For completeness, Whaleco would add that it deploys extensive mitigation measures aimed at ensuring that illegal products are not listed on Temu. These are described in the Product Compliance, IP, and Content Compliance module, and they benefit minors accessing Temu in the same way as they benefit adult users. As mentioned above in this section, Temu's text and image recognition algorithms automatically screen all product information provided by traders, and a manual review may then be carried out by trained human specialists experienced in identifying prohibited products.

ii. Mitigation measures addressing risks stemming from Temu's services and features

Beyond its core marketplace functions, Temu provides additional services and features—such as product reviews, search, interactive activities, and the A&I Programme—that may expose minors to distinct risks. Whaleco has therefore embedded safeguards in the design and operation of these features to prevent exposure to harmful or age-inappropriate content, to ensure clarity in promotional experiences, and to enforce trader compliance with Temu rules. These measures, which build on the consumer protection framework described earlier, are tailored to the heightened vulnerabilities of minors and seek to mitigate risks without undermining Temu's primary purpose as an adult-oriented service.

a. Mitigation measures addressing risks stemming from Temu's facilitation infrastructure

Risk category	Mitigation measures addressing risks stemming from Temu's facilitation infrastructure
Content risks	**Strict policies addressing CSAM content listings.** Whaleco has strict policies and procedures towards traders regarding illegal content, which is further described in the Illegal Content, Product Compliance and Intellectual Property module. Addressing CSAM, Temu's Product Safety and Compliance Policy explicitly prohibit "*Content or information related to pornography involving minors, non-consensual or paid sex, or other illegal sexual themes*" Temu screens for this prohibited content in its dedicated product listing process by leveraging image and text recognition models, which include image recognition of historically banned content. It also employs multi-factor analysis and algorithmic identification to identify potential CSAM content. Temu blocks or delists the content and, if the trader is at fault, warns or penalises the trader. For any trader found to have listed CSAM content, Temu applies strict penalties. These include the immediate removal of the relevant products, permanent closure of the store, and termination of the trader's account. **Moderation and user reporting of product reviews**. As described in the Consumer Protection module, all submitted reviews undergo automated screening before they become publicly visible. [Confidential] On the user side, Temu provides an easily accessible reporting function on each product page that allows users to flag problematic content on Temu for a manual review by the moderation team. In the "Report this Review" function, users can check a box that directly indicates CSAM. In line with European regulation, it allows reporting on the basis that the "*Review concerns sexual abuse, sexual exploitation of children, or child pornography*" followed by the option to "*Check this box if the content reported involves one of the offences referred to in Article 3 to 7 of Directive 2011/93/EU (including sexual abuse and sexual exploitation of children and child pornography)*" During the Relevant Period, Temu received [Confidential] reports of potential CSAM from EU users, and the average time taken from notification to take-down was [Confidential] hours. Considering that this process involves a full manual evaluation of the content involved, a resolution time of less than [Confidential] hours indicates an effective process. **Restrictions on inappropriate search terms**. Temu has adopted a mechanism to block and blacklist any non-compliant search keywords

Risk category	Mitigation measures addressing risks stemming from Temu's facilitation infrastructure
	(for example, child abuse, child pornography, and others) entered by users. If a user inputs a blacklisted term or keyword in the search bar, the mechanism will prevent the display of recommended keywords in the drop-down suggestions menu, and no search results will be returned. Temu continuously optimizes this mechanism, including by deploying deep learning technologies, to block variations of blacklisted keywords.
Contact risks	**Enforcement of trader policies**. Whaleco considers that the technical limitation on communications between traders and users is largely sufficient to address the risk to minors. It includes provisions in its trader contracts regulating how traders communicate with users and relies on enforcement of these provisions to address any remaining risk. For example, the Seller Code of Conduct includes prohibitions on making false representations in relation to the availability of products, or availability on particular terms, withholding information from a consumer that is essential for an informed business decision, and requires traders to communicate with buyers in a respectful manner, without offensive or abusive language which may contain personal attacks or insults.

b. Mitigation measures stemming from Temu's promotional activities

Risk category	Mitigation measures addressing risks stemming from Temu's promotional activities
Consumer risks	**Exclusion of adult-only products.** Temu controls the content of its interactive activities at all times and does not proactively include adult-only products through its interactive activities or coupons. Adult-only product categories such as sexual wellness products are not proactively recommended to users provided that they have not searched for such products previously. This lowers the chance of minors being exposed to and therefore purchasing such products. **Warning labels and age-gating**. As described earlier, the risk that minors may be able to purchase age-inappropriate products is mitigated by a series of measures including warning labels and age-gating.
Cross-cutting risks for health and well-being	**Built in compliance review for minor protection-related features.** As described earlier in the Consumer Protection module, before the introduction of product features and promotional interactive activities, and on a regular basis thereafter, these features and activities undergo review by a dedicated internal compliance team. This is where minor protection is proactively assessed in Whaleco's "compliance-by-design" multi-stage approach. Minor protection-related features such as age-gating features or warning labels are implemented, and terms and conditions relating to minors are ensured to be compliant with Whaleco standards and any relevant legal requirements. [Confidential]

iii. Mitigation measures tailored to Article 34(2) influencing factors

In line with Article 34(2) of the DSA, Whaleco has taken steps to mitigate risks linked to recommender systems and data-related practices related to minors. For content risks relating to recommender

systems, this includes restricting age-inappropriate content from proactively being shown, restrictions on inappropriate search, and product listing safeguards before being displayed to the consumer. For consumer risks relating to data-related practices, this includes Temu's Privacy Policy regarding minors specifically, limited permissions by design, and parental deletion of minors' accounts.

Risk category	Mitigation measures tailored to Article 34(2) influencing factors
Content risks	**No adult-only products proactively recommended through the product recommender system.** As previously mentioned, Temu controls the content of its promotions at all times and does not proactively promote adult-only content through its interactive activities or coupons. In line with this design, adult-only product categories such as sexual wellness products are excluded from Temu's recommender systems except where the user has previously searched for such products. Temu also does not promote adult-only product categories through its interactive activities or coupons. **Product listing safeguards pre-display.** With respect to potentially unsafe or adult-only products that might be presented to minors through product recommendations, Temu adopts mitigations acting at any earlier stage, in relation to product listings, as a preventative approach. These are described in more detail in the Illegal Content, Product Compliance and Intellectual Property module.
Consumer risks	**Privacy Policy towards minors.** In Temu's Privacy Policy, there is an entire section clearly labelled and dedicated to minors: "*Children - The Service is not intended for use by anyone who is under the age of 18 or a minor (as defined by applicable law). If you are a parent or guardian of a child about whom you believe Whaleco has collected personal information, please contact us directly or through its online reporting form. If Whaleco learns that it has collected personal information through the Service from a child or without the knowledge of a child's parent or guardian as required by law, Whaleco will comply with applicable legal requirements to delete the information*." This was last updated on 6 August 2025 to reflect the evolving regulatory requirements. **Limited permissions collected.** In the user account - Permissions section, Temu explicitly states in a clearly disclosed and visual and accessible way the following information, where it in fact does not collect many types of personal data: "*The Temu App DOES NOT access the following device features: Microphone, Bluetooth, Photos (The Temu App does not access your photos. You can still use your device's system's built-in image picker when leaving a review, searching for items, etc., without Temu accessing your photos.), Contacts, Clipboard, Location, Others. (In addition to the above permissions, The Temu App will not access any other permissions, such as calendars, etc.)*". **Parental deletion of minors' data**. Temu's recommender systems are limited to user data generated on Temu itself. This does not include age-related data, and, since Temu consists of a marketplace intended for product purchases, the data that is collected provides only very limited insights into a user's private life. Nonetheless, as described earlier, Temu provides an easy-to-use online reporting form enabling parents and guardians to request deletion of any Temu account that their child has managed to open. Temu will destroy all user data associated with that

Risk category	Mitigation measures tailored to Article 34(2) influencing factors
	account, preventing it from being used to target the minors concerned with personalised product or promotional recommendations.

D. Residual Risks and Future Mitigation Measures

Based on Whaleco's implementation of controls in relation to the risks for minors arising from Temu's core characteristics as well as its services and features, Whaleco assesses the residual risk as "**Medium**".

Module	Inherent Systemic Risk	Control Strength	Residual Risk
Minor Protection	Medium-High (4/5)	Somewhat Effective (3/5)	Medium (3/5)

To address the residual risks and potential insufficiencies of the existing mitigation measures identified in the Year 2 risk assessment, Whaleco plans on enhancing the mitigation controls against consumer protection risks in the following areas:

Mitigation Type	Description (DSA Article 35)	Controls	Control Enhancement Description
Internal Risk Management & Oversight	Taking targeted measures to protect the rights of the child, including age verification and parental control tools, tools aimed at helping minors signal abuse or obtain support, as appropriate	Product Age-Gating	Explore enhanced solutions for age-restricted products that are inappropriate for minors under relevant EU laws, including third-party verification mechanisms and any age-verification solutions to be introduced by the European Commission.
Internal Risk Management & Oversight	Reinforcing the internal processes, resources, testing, documentation, or supervision of any of their activities in particular as regards detection of systemic risk	A&I Programme	Enhance age restrictions in relation to influencers enrolling in the A&I Programme by requiring them to verify their adult status through a pop-up window during application processes. This requirement will further enhance existing preventative mitigation measures towards protection of minors.
External Engagement	Adapting the design, features or functioning of services, including their	Stakeholder Engagement	Whaleco will continue to maintain ongoing engagement with relevant European Union institutions, regulatory bodies, and industry stakeholders on matters pertaining to minor protection

Mitigation Type	Description (DSA Article 35)	Controls	Control Enhancement Description
	online interfaces; adapting terms and conditions and their enforcement		law and policy. This proactive engagement will include consultations and structured dialogue aimed at understanding evolving regulatory expectations, as well as forthcoming practical initiatives such as the age verification solutions. This commitment ensures Temu's compliance strategies are aligned with the dynamic EU regulatory landscape, thereby supporting consistent regulatory compliance and promoting fair practices.

IX. Fundamental Rights

Article 34(1)(b) of the DSA requires **VLOPs** to assess whether, when operating their platforms, there would be any actual and foreseeable systemic risks to the exercise of fundamental rights protected under the Charter of Fundamental Rights of the EU, including the rights to human dignity, the protection of personal data, the principle of non-discrimination and the right of freedom to conduct a business.

This module (i) identifies and assesses the potential systemic risks of fundamental rights infringements on Temu, (ii) describes their potential impact absent any mitigation measures, and (iii) cross-references the tailored mitigation measures Temu has adopted to address such risks. The systemic risk environment for fundamental rights is dynamic and evolves each year in response to new political, regulatory and legal developments, which could also impact the products offered by traders on Temu. This means that the risk assessment and respective mitigation measures to address actual and foreseeable negative effects on the fundamental rights of users are constantly under review. Actual and foreseeable effects on the right to consumer protection, including minor protection, have been assessed separately in **Sections VII and VIII** of this Report.

During the Relevant Period, the systemic risk environment for fundamental rights has been broadly consistent with what is outlined in the Product Compliance, IP, and Content Compliance module (see **Section VI** of this Report). While the assessed attributes (and their related systemic risk environment) for fundamental rights during the Relevant Period show a similar probability, the overall risk severity rating for fundamental rights is considerably lower. This is because, in spite of the underlying attributes and potential risk factors being similar, the actual adverse effects on fundamental rights appear to be less severe in practice.

A. 2025 Highlights

During the Relevant Period in Year 2, Whaleco implemented several key changes to strengthen its risk assessment and compliance with fundamental rights requirements under Article 34(1)(b) of the DSA. This included stricter identity and business registration checks, as well as mandatory acceptance of updated contractual obligations such as the Seller Code of Conduct and the Prohibited Products List, both of which explicitly reference fundamental rights standards.

In addition, the appeals process for content removals was enhanced to provide a clearer SOR and more accessible and timely review procedures, in line with Article 17 of the DSA. Engagement with external stakeholders, including consumer organisations and regulatory authorities, led to further refinements to both proactive and reactive mitigation measures. These include regular updates to moderation rules for high-risk product categories and the integration of stakeholder feedback to ensure that Temu's approach to fundamental rights compliance remains responsive to evolving legal and societal expectations.

Below is a snapshot of Whaleco's risk assessment results.

Module	Inherent Systemic Risk	Control Strength	Residual Risk
Fundamental Rights	Low-Medium (2/5)	Mostly Effective (4/5)	Low (1/5)

B. Assessment of the Systemic Risks

Article 34(1)(b) and Recital 81 of the DSA provide that the risk assessment should consider any actual or foreseeable negative effects on the exercise of fundamental rights, in particular the rights to human

dignity, the respect for private and family life, the protection of personal data, the right to freedom of expression and information, the right to non-discrimination, respect for the rights of the child and consumer protection.

While the DSA requires Whaleco to consider the full range of fundamental rights, their specific applicability varies depending on the nature of the online service. Temu is an online marketplace where third-party traders can sell products to consumers in the EU. Importantly, Temu does not provide social networking services (i.e., peer-to-peer connection). The content included on Temu (e.g., product information and product reviews) is rather commercial in nature, be it with regard to product information and product reviews (generated by traders and consumers respectively) or sales events and promotional content (generated by Temu). This design limits both the scope of foreseeable negative effects and the potential impact on fundamental rights, as well as the particular fundamental rights that can be affected. Whaleco considers there to be systemic risks in four main categories as described below:

- **The right to Human Dignity (Article 1 of the Charter of the Fundamental Rights of the EU):** The right to human dignity is rooted in the belief that every individual possesses inherent worth and value simply by being human, regardless of such individual's race, gender, status, or any other characteristic, and is therefore entitled to respectful treatment.

- **The right to Private and Family Life and the Right to Protection of Personal Data (Articles 7 & 8 of the Charter):** Articles 7 and 8 of the Charter protect the rights to private and family life and personal data.

- **The right to Freedom of Expression and the Right to Conduct a Business (Articles 11 & 16 of the Charter):** Article 11 of the Charter protects the freedom of expression, while Article 16 protects the right to conduct a business. These rights ensure people can share ideas and run businesses without unfair restrictions imposed by governments or intermediaries and platforms.

- **Right to Non-Discrimination, Equal Treatment and integration of persons with disabilities (Articles 21 & 26 of the Charter):** Article 21 of the Charter bans discrimination based on factors such as sex, race, disability, age, or sexual orientation. Article 26 of the Charter requires support for the inclusion of people with disabilities.

The Protection of Minors and Consumer Protection modules are addressed separately; they are discussed only insofar as they interfere directly with the identified risks in the scope of this section. Therefore, this section does not cover them as a separate analysis (see, in that sense, **Sections VII and VIII**).

i. Core Characteristics

Each of Temu's core characteristics, i.e., (1) hosting traders, (2) hosting product listings, (3) accommodating EU users, and (4) facilitating online marketplace sales, can give rise to certain systemic risks related to the four fundamental rights categories at issue or influence the probability or severity of the risks.

The right to Human Dignity (Article 1 of the Charter of the Fundamental Rights of the EU): On Temu, several inherent systemic risk scenarios regarding the right to human dignity may arise in the absence of effective mitigation measures. One such risk is the listing of degrading products, which may include hate materials or humiliating depictions. The failure to remove or prevent the sale of such products can directly undermine the principle of human dignity. Furthermore, the hosting of Temu's trader network

generates a high volume of product listings and descriptions. This creates a systemic risk that prohibited or degrading products or content could appear on Temu. In addition, certain product categories, such as adult products, food and drugs, carry an inherently higher risk profile due to their sensitivity and stricter regulatory requirements. These risks implied could affect the right to human dignity (Article 1 of the Charter, see also **Section VII**). Temu's design may present risks related to over-gamification or the presence of potential dark pattern elements, which could contribute to shopping addiction. These design-related risks, particularly as they pertain to consumer and minor protection, are addressed in greater detail in **Sections VII and VIII**. During the Relevant Period, Temu received 840 notices against non-compliant contents from the review function and 1,991 notices against products from users for reasons that are related to issues concerning the following topics: (i) violence, (ii) cyber violence, (iii) cyber violence against women, (iv) data protection and privacy violations, and (v) illegal or harmful speech, all of which Temu considers to be connected to the protection of fundamental rights ("**Fundamental Rights-related**"), with a median response time for these notices not exceeding 24 hours. Out of these Fundamental Rights-related notices, 109 notices against non-compliant contents from the review function and 81 notices against products resulted in content-disabling action being taken by Temu. In addition, with regard to Temu's large trader network, [Confidential] of trader applications were rejected following comprehensive due diligence, further mitigating the risks of bad actors infringing consumers' right to human dignity.

The right to Private and Family Life and the Right to Protection of Personal Data (Articles 7 & 8 of the Charter of Fundamental Rights of the EU): Operating an online marketplace, through which traders are connected with consumers for the sale of products, requires the processing of personal data and the use of certain cookies and similar technologies (e.g., to save items for a certain period of time in the shopping cart) (e.g., Cookies and Similar Technologies Policy). Unlawful or excessive processing of personal data–including profiling, targeted advertising, and behavioural tracking–can reveal sensitive aspects of users' private lives. Additional concerns involve inadequate protection of minors from adult content, the inclusions of personal data in the review section, data breaches due to weak security measures (and the failure to meet notification obligations under the GDPR), or phishing or impersonation attempts targeting users' data. During the Relevant Period, Temu recorded more than [Confidential] instances of users rejecting all non-essential cookies, indicating accessible controls and ease of exercising choice. Where a user takes no action when the cookie banner appears, non-essential cookies are rejected by default. During the Relevant Period, approximately 10% of user notices received in respect of potential data protection and privacy violations in reviews resulted in takedowns. Temu reviewed these notices with a median processing time of less than 14 hours.

The right to Freedom of Expression and the Right to Conduct a Business (Articles 11 & 16 of the Charter of Fundamental Rights of the EU): Disproportionate or inadequate content controls or unclear rules can illegitimately limit business opportunities. Other risks include non-transparent content moderation, account suspensions or product takedowns without clear justification, as well as overenforcement of such measures. Inadequate appeal or redress mechanisms may limit users' right to an effective remedy, and over-removal of legitimate product listings can unduly restrict lawful speech and commercial activity. During the Relevant Period, trader appeals were processed with a median turnaround of approximately 48 hours; approximately 200 Fundamental Rights-related product moderation actions were reconsidered and successfully reinstated.

The right to Non-Discrimination, Equal Treatment and integration of persons with disabilities (Articles 21 & 26 of the Charter of Fundamental Rights of the EU): In the absence of effective safeguards, risks may arise such as accessibility barriers that prevent equal participation by persons with disabilities, Temu features that do not accommodate diverse needs, and discriminatory content in product listings or contents, caused and amplified by Temu's large trader network, that is not adequately addressed. A similar risk profile can be found for product descriptions by traders. Risks can also relate to Temu's EU user-base, which includes users from diverse linguistic and cultural

backgrounds, as well as vulnerable groups such as minors (see **Section VIII).** As for the right to human dignity, certain vulnerable groups of people may face difficulties accessing the platform. To monitor and address this risk, Whaleco has proactively carried out a range of accessibility improvements, outlined in our Accessibility page, to its service and separately engaged an independent accessibility compliance auditor to assess these measures. These efforts include keyboard navigation support, screen reader compatibility, and zoom and display adjustments.

ii. Services and features

Building on the description of the risk factors and Temu's core characteristics described in **Section IV**, this subsection provides an overview of Temu's functionalities that may influence risks related to fundamental rights. Each feature is assessed in line with the methodology set out in **Section III**.

- **Limited chat functions:** Temu's trader-to-consumer chat is limited to transactional purposes, which inherently restricts the risk of rights-infringing behaviour such as harassment, discriminatory language, or privacy violations. The private, one-to-one nature of the interface means that any abuse is isolated and not scalable. Potential impacts include infringements on human dignity (Article 1 of the Charter of the Fundamental Rights of the EU), privacy (Article 7 of the Charter), and non-discrimination (Article 21 of the Charter), but the absence of public or group messaging and the exclusion of consumer-to-consumer chat significantly reduce the likelihood of systemic risk. The chat function is not available on product listing pages or store homepages, and traders cannot initiate the chat.

- **Risks related to on-platform promotional activities:** On-platform promotional activities, including rewards and curated events, may slightly increase fundamental rights risks by incentivising excessive purchasing or disproportionately affecting vulnerable users, but these programmes are voluntary, capped, and do not involve credit or debt. The main rights at risk are the protection of minors (Article 24 of the Charter) and consumer protection (Article 38 of the Charter). The risk is higher if non-compliant products are featured in promotions, as this amplifies their reach and impact. The probability of harm depends on curation quality, with human oversight reducing risk.

- **Risks related to off-platform promotional activities:** The A&I Programme increases the risk that infringing content—such as misleading, discriminatory, or harassing commentary—may be disseminated beyond Temu's direct control. The use of off-platform promotions complicates the ability to trace and monitor the content and methods of advertising, increasing the risk that infringing material may be disseminated without oversight. This can affect rights to dignity (Article 1 of the Charter), equality and non-discrimination (Article 21 of the Charter) and consumer protection (Article 38 of the Charter). Key risk drivers include the difficulty of monitoring external content and the potential for influencers to introduce problematic material. The Affiliate Policy and The Influencer Policy further elaborate on the fundamental rights-related risks related to off-platform promotions.

iii. DSA 34(2) influencing factors

In line with Article 34(2) of the DSA, Whaleco has considered the specific impact of the outlined factors on potential breaches of fundamental rights. Only the factors deemed relevant are covered. For a more elaborate analysis, Whaleco refers to **Section VI.**

Data-related practices and recommender systems: The collection and processing of personal data on Temu—particularly through recommender systems—introduces systemic risks to privacy and non-discrimination. The scale of data collected from a large user base, combined with the diversity of

features for which data is used, increases the probability of misuse, insecure storage or unfair processing. These risks can result in privacy breaches, discriminatory profiling or large-scale harm, with user data being especially susceptible due to its potential for misuse and security breaches. In addition, recommender systems can influence exposure to harmful or discriminatory content and may impact privacy through their data use. The risk level depends on the design and operation of these systems. During the Relevant Period, Temu recorded more than [Confidential] instances of users rejecting all non-essential cookies, indicating accessible controls and ease of exercising choice. Where a user takes no action when the cookie banner appears, non-essential cookies are rejected by default. Approximately 10% of user notices received in respect of potential data protection and privacy violations in reviews resulted in takedowns, with a median processing time of less than 14 hours, while Temu's content moderation systems detected and removed more than 43,000 instances of potential data protection and privacy violations against non-compliant contents from the review function.

Content moderation systems: An adequately enforced content moderation system supports fundamental rights, amongst others, by protecting users' right to human dignity (Article 1 of the Charter of the Fundamental Rights of the EU) and ensuring non-discrimination (Article 21 of the Charter) through the removal of harmful or unlawful content. However, excessive or inaccurate enforcement can negatively impact the right to freedom of expression (Article 11). On Temu, this risk is limited in scope, as Temu is not content-based and moderation primarily targets product listings rather than user-generated social content.

Applicable Terms and Conditions and their Enforcement: The main legal documents governing Temu—including the Terms of Use, Community Guidelines, Privacy Policy, Seller Code of Conduct, and Seller EU Services Agreement — present a risk that users may potentially limit their exercise of fundamental rights, particularly if the terms are ambiguous or complex to access. While legal paperwork that lacks qualitative safeguards increases the likelihood of rights being affected, Temu's T&Cs are structured to inform users, set boundaries for good conduct, and provide a legitimate basis for content moderation without undermining legal certainty. Rights potentially affected include the right to information and informed consent, the right to redress and effective remedy (Article 47 of the Charter of the Fundamental Rights of the EU), freedom of expression (Article 11 of the Charter) and non-discrimination (Article 21 of the Charter).

Inherent systemic risk evaluation

The overall inherent systemic risk for the Fundamental Rights module is assessed as "low-medium". The inherent systemic risk assessment evaluates the probability and severity of systemic risks in the hypothetical absence of any mitigation measures.

Sub-module	Inherent Systemic Risk Score	Assessment Findings
Fundamental Rights	**Low–Medium**	**Probability (Medium-High - 4/5):** For fundamental rights, a medium historic occurrence of systemic risks on Temu, combined with medium-high occurrences observed on other VLOP marketplaces and reflected in market research and regulatory indications, results in a medium-high probability score.

Sub-module	Inherent Systemic Risk Score	Assessment Findings
		Severity (Low-Medium - 2/5): For fundamental rights, the potential severity of the inherent risk is considered low-medium. This is due to a low number (3.54%) of total user reports being related to fundamental rights, leading to a medium-low assessment of scope and remendability and a medium assessment of scale. Ultimately, there is no evidence that Temu's features and services have inflicted fundamental rights-related harm to Temu's users.

C. Mitigation Measures

Building upon Whaleco's identification, analyses, and assessment of how Temu's core characteristics, services, and features influence its inherent systemic risks of fundamental rights infringements, Whaleco has developed a framework of mitigation measures. While these measures address risks common to all modules, certain safeguards have particular relevance in relation to the inherent systemic risks of fundamental rights infringements.

The following subsections provide a detailed analysis of the multi-layered system of policies, controls, and monitoring mechanisms implemented by Whaleco that contribute to mitigating risks of fundamental rights infringements, along with representative performance metrics that demonstrate their effectiveness where available. This builds on the description and assessment of the mitigation measures in previous parts of this Report, more specifically in **Section V** and **Section IV**.

Given the systematic evaluation of mitigation measures tailored to address the risks of fundamental rights infringements, Whaleco considers the overall effectiveness of its controls for fundamental rights to be **Mostly Effective.**

i. Governance, Risk & Compliance (GRC) oversight

Whaleco's GRC framework is managed by a dedicated Trust & Safety team that combines automated detection with rapid response mechanisms to handle signals from internal systems as well as reports from users, regulators, rights-holders and trusted flaggers under Article 22 of the DSA. The system applies through the same mechanisms and methodologies as explained in **Section V** and **Section VI.**

ii. Policies & Standards

Whaleco provides for a set of Policies & Standards that contain binding safeguards which oblige both traders and users to refrain from listing or sharing infringing, unsafe, or non-compliant content on Temu (see **Section V** and **Section IV**). In addition, Whaleco has adopted an integrated data protection framework to ensure Temu, its traders, and users comply with relevant data protection rules and the right to privacy.

The table below summarises and analyses the mitigation measures that have specific relevance for risks of fundamental rights infringements.

Risk category	Control Descriptions: Policies & Standards
Fundamental Rights	**1. Overview** **(1) Content infringing fundamental rights** Whaleco's fundamental rights compliance framework borrows from various policies relating to product compliance and content compliance to mitigate the fundamental rights risks associated with product listings and trader and user content. Temu's Terms of Use contain the rules and restrictions that govern the use of Temu's applications, products, services and websites by users. They bind users to the Community Guidelines and the Review Guidelines, which explicitly prohibit content that is hateful, discriminatory, harassing, or invades privacy. The Terms of Use also contain an enumeration of products and content that is prohibited on Temu, including products and content that violates fundamental rights, as part of Temu's Product Safety and Compliance Policy. This framework is supported by a Temu Seller Code of Conduct, which contains a set of principles relating to ethical, humane, and lawful business practices. Anyone conducting business directly on Temu must ensure their and their suppliers' strict compliance with this Code of Conduct and with all applicable local, national, and international laws, including also fundamental rights. In case of incompliance, enforcement action is taken. During the Relevant Period, more than 390,000 proactive measures were taken against products and more than 48,000 were against non-compliant contents from the review function for Fundamental Rights-related violations. Whaleco also provides an easy-to-use report button for users to report violations and action reactive user reports promptly. The median time to action user notices alleging Fundamental Rights-related violations does not exceed 24 hours during the Relevant Period. **(2) Data protection** In addition, Temu's data protection framework is based on four pillars: (1) Limited and Consent-Based Data Processing: Collecting only necessary data based on user consent and for specified purposes, as outlined in its user Privacy Policy; (2) Transparent Policies: Providing clear, accessible information to users about what data is collected and how it is used within our Privacy Policy ; (3) Robust Data Security: Implementing a comprehensive suite of technical and organisational security measures, including encryption, access controls, and vulnerability management and (4) Privacy Choices: Offering users granular controls over their data and marketing preferences via the Your Privacy Choices page. Feedback from user requests and stakeholder engagement is used to adapt and improve its privacy policies and practices. Temu provides toggle with the Your Privacy Choices page that allow users to turn off personalised recommendations, and a dedicated page for submitting Data Subject Requests (DSRs) that is clear, accessible, and easy to use. More than 12,000 users had opted out of their personalised recommendation setting as of June 30, 2025, demonstrating ease for users to exercise their choice of turning off personalised recommendations. Temu offers easy access to users if they want to delete their account, accessible via the "Account security" section of user's profile settings. Temu allows users a reasonable period of seven days to reconsider their decisions, after

Risk category	Control Descriptions: Policies & Standards
	which we will promptly delete the user's account per request. During the Relevant Period, Temu received approximately [Confidential] account-deletion requests, with an average completion time of about eight days, counting the seven-day period, of which [Confidential] resulted in the completion of deletion request. The remaining requests were not completed because users chose not to proceed. **2. Qualitative assessment** Whaleco considers the residual risk of fundamental rights violations to be low following the application and enforcement of its Policies and Standards, in particular because (i) Temu is not a social media platform, (ii) Whaleco provides traders with onboarding training, which includes training on fundamental rights, (iii) Whaleco automatically screens new product listings for harmful content, including fundamental rights violations, and (iv) Whaleco has high-performance proactive detection mechanisms, which is demonstrated inter alia by the relatively low number of user notices compared to the own detection violations. Furthermore, regarding data protection and privacy in particular, Whaleco considers, based on the application and enforcement of its data protection framework, the residual risk to be low as, next to the low residual risk of fundamental rights infringements in general, (i) Temu is not focused on collecting user data (limited and consent-based data processing, privacy choices), (ii) Whaleco applies robust data security measures and (iii) Whaleco strives to keep reaction times to data subject requests and user reports alleging privacy violation low. There is, however, a limited risk that users may be exposed to fundamental rights infringements during the reaction times in responding to user reports. Whaleco will continue to improve its reaction times to limit the risk of exposure to fundamental rights infringements. Similarly, Whaleco strives to further improve its reaction times to data subject requests.

iii. User Management & Onboarding Control

Temu has established a rigorous trader onboarding and vetting system designed to ensure compliance and credibility from the outset, including with fundamental rights (see **Section V** and **Section VI**).

The table below summarises and analyses the mitigation measures that have specific relevance for risks relating to fundamental rights infringements.

Risk category	Control Descriptions: User Management & Onboarding Control
Fundamental Rights	**1. Overview** As part of the **onboarding obligations**, all traders must accept the Seller Code of Conduct, which explicitly outlines their responsibilities regarding fundamental rights. A violation of this code may result in a suspension or ban from Temu. Training materials, provided during trader onboarding and available to all traders in the Seller Center, inform traders about Temu's rules about prohibited products and content, including that noncompliance may result in potential violations of users' fundamental rights. Following onboarding, Whaleco invests in continuous trader education to ensure ongoing compliance. Its dedicated online Seller Education Programme has generated over 8 million views during the Relevant Period. In addition to self-learning resources, Whaleco delivers high-impact initiatives such as a recurring monthly training series, organised in partnership with the EU consumer protection organisation SPEAC, to strengthen trader compliance awareness. **2. Qualitative assessment** Whaleco considers the residual risk of fundamental rights violations to be limited following the application and enforcement of these mitigation measures. This is in particular because of (i) high compliance rates of newly onboarded traders and (ii) the relatively low number of user reports and own initiative measures relating to fundamental rights infringements, demonstrating general compliance of traders with fundamental rights. Whaleco does acknowledge, however, that within the fundamental rights categories, the number of user reports and own initiative measures are relatively high for illegal or harmful speech. Whaleco will strive to bring these numbers further down by paying more attention to this specific kind of fundamental rights infringement during onboarding and training.

iv. Detection & Enforcement

Whaleco has established a multi-layer content moderation framework that integrates automated detection with human review (see **Section V** and **Section VI**). It also provides a specific procedure for data incidents.

The table below summarises and analyses the mitigation measures that have specific relevance for risks relating to fundamental rights infringements.

Risk category	Control Descriptions: Detection & Enforcement
Fundamental Rights	**1. Overview** Whaleco applies proactive screening of trader-uploaded content for potential violations of fundamental rights. Whaleco employs a combination of automated tools and human review to monitor for potentially infringing content. Certain content may be referred for manual assessment where additional review is considered appropriate. Whaleco also conducts regular, mandatory training sessions on specific topics for human reviewers. Furthermore, the Temu Product Safety and Compliance Policy contains category-specific rules that ban items which are inherently likely to infringe on fundamental rights. During the Relevant Period, more than 390,000 proactive measures were taken against products and more than 48,000 were against non-compliant contents from the review function for Fundamental Rights-related violations. In relation to data protection, Whaleco has an incident management procedure to investigate, respond to, and mitigate any potential data breaches. **2. Qualitative assessment** Whaleco considers the residual risk of fundamental rights violations to be limited following the application and enforcement of these mitigation measures, in particular because of (i) the effectiveness and accuracy of its automated own detection mechanisms and (ii) the relatively low overturn rate of content disabling measures on notices. The low but persistent number of fundamental rights infringements established following user notices suggests that there is still a limited risk of exposure to fundamental rights infringing content. Whaleco will strive to review its procedures in relation to these types of decisions and seeks to bring down median response time to limit the impact of these decisions on the fundamental rights of the users concerned.

v. User Rights and Remedies Mechanisms

Temu has established clear and accessible feedback and complaint channels, ensuring that every user (including traders) affected by Whaleco's decisions has a direct avenue to be heard and can seek a remedy (see **Section V** and **Section VI**).

The table below summarises and analyses the mitigation measures that have specific relevance for risks relating to fundamental rights infringements.

Risk category	Control Descriptions: User Rights and Remedies Mechanisms
Fundamental Rights	**1. Overview** Temu provides a notice and action mechanism following which all recipients of services, including both logged-in and non-logged-in users, may report potentially fundamental rights infringing products through the "Report this Item" feature. The "Report this Item" button is prominently displayed on each specific product listing page, ensuring ease of access. These reports are handled by human moderators. When Temu determines

Risk category	Control Descriptions: User Rights and Remedies Mechanisms
	that a report is unfounded or when restrictive measures are imposed, affected recipients are automatically notified. Each restriction measure is subject to a SOR, which is (i) aligned with the specific nature of the infringement for which the restriction measure is imposed and (ii) based on the prohibited fundamental rights related content and behaviour set out in the Community Guidelines (for example, Articles 3, 5 and 6). The content of each SOR is generated from pre-configured templates corresponding to the specific category of enforcement, ensuring accuracy and consistency in all notifications. The templates used to generate these SORs are based on the factors set out in Article 17 of the DSA. Each notification also contains a user-friendly appeal link, allowing recipients to challenge the decision. The internal appeals mechanism provides for the review of measures *inter alia* taken in respect of alleged fundamental rights infringements. It also serves as a remedy against measures taken in respect of other types of infringements, allowing for a fair review in line with applicable standards. Further to this, in relation to data protection, Temu provides for dedicated channels for users to exercise their data subject rights, such as requests for access or deletion via a dedicated web page or by contacting the privacy team. During the Relevant Period, Temu received 840 notices related to non-compliant contents from the review function and 1,991 notices related to products from users in respect of Fundamental Rights-related issues, with a response time for these notices not exceeding 24 hours. Out of these notices, 108 review-related notices and 81 product-related notices resulted in content-disabling action being taken. Approximately 10% of user notices received in respect of potential data protection and privacy violations in reviews resulted in takedowns. **2. Qualitative assessment** Whaleco considers the residual risk of fundamental rights violations to be limited following the application and enforcement of these mitigation measures, in particular because of (i) the automatic and reasoned notification of negative decisions, (ii) the easy access to the internal appeals mechanism and (iii) the effectiveness and impartiality of the internal appeals process, demonstrated by various overturn rates show Temu will strive to bring down median appeal durations against negative decisions, especially negative decisions relating to the suspension or termination of accounts, given the impact of such decisions on the fundamental rights of the traders concerned.

vi. External Engagement

Whaleco refers to **Section V** and **Section VI** for a description of its External Engagement in general. The table below summarises and analyses the mitigation measures that have specific relevance for risks relating to fundamental rights infringements.

Risk category	Control Descriptions: External Engagement
Fundamental Rights	**1. Overview** Whaleco engages with consumer organisations such as BEUC and takes into account feedback and reports from such bodies to inform and adapt policies and enforcement practices related to Temu's risks, including those concerning fundamental rights. By way of an example, Whaleco refers to its engagement with BEUC following its May 2024 report on Temu as well as its proactive outreach to 17 member organisations of BEUC to understand their concerns (see **Section VIII**) **2. Qualitative assessment** Whaleco considers the residual risk of fundamental rights violations to be limited following the application of these mitigation measures, in particular because its external engagement (i) leads to actual changes in its policies directly discussed with relevant stakeholders and (ii) takes the form of a continuous dialogue that allows for a constant feedback loop.

vii. Other Mitigation Measures Addressing Specific Influence Factors

In addition to the mitigation measures structured under the defined control domains, Whaleco has established dedicated control mechanisms targeting identified risk-influencing factors (see **Section IV**) that could amplify Temu's exposure to non-compliant content dissemination, including fundamental rights-infringing content. These measures primarily focus on the recommender systems, the A&I Programme, and controls designed to prevent the reappearance of non-compliant products.

Service & function	Control Descriptions
Recommender system	Temu's recommendation system operates exclusively on products that have already passed compliance reviews. The primary residual risk arises from the possibility that a small number of non-compliant products, including fundamental rights infringing products, may enter the recommendation pool due to occasional review oversights. This risk is mitigated by the application of blocked search terms, following which the search algorithm is proactively mitigated by blocking certain hateful or discriminatory terms. Additionally, user controls allow individuals to reactively shape their own feed. Regarding data protection, the DSA Help Page and Privacy Policy inform users about how the recommender system works and what data is used. Further to this, Temu's principles of limited and consent-based data processing apply. This implies that its systems are designed to use a limited set of data necessary for personalisation, and sensitive data is not collected, minimising privacy intrusion.

Service & function	Control Descriptions
On-platform promotional activities	Any product is subject to standard content moderation before it can be considered for a promotion. This is designed to filter out infringing content at the source, including fundamental rights infringing content. In case a product in a promotional slot is identified as infringing (e.g., via user reports), the immediate reactive step is to remove it from the promotion, in addition to taking down the product listing itself. An incident of this nature would trigger a reactive review of the curation process to identify and rectify any gaps that allowed the product to be selected.
Off-platform promotional activities	In addition to the mitigation measures applied to on-platform promotions (content moderation, internal curation process, user reports), Temu Affiliate Policy and Temu Influencer Policy bind all participants to the A&I Programme to a code of conduct that sets rules for their promotional activities, providing a basis to prohibit fundamental rights infringing behaviour.

D. Residual Risks and Future Mitigation Measures

The residual risk is the level of systemic risk remaining after the implementation and evaluation of the mitigation measures detailed in the preceding **Section IX.**

For this assessment, Whaleco considered two dimensions:

- **Inherent systemic risk**: this concerns the likelihood of recurrence of infringements (frequency of infringements observed in the Relevant Period) and the severity of harm to fundamental rights if infringements occur; and

- **Control effectiveness**: the extent to which current measures demonstrably reduce risk, based on a qualitative analysis and supplemented with performance metrics where available.

While proactive detection systems catch more than 99% of content resulting in Fundamental Rights-related infringements, a limited number of residual instances of discriminatory or rights-violating content continue to appear. This indicates a very low but persistent level of attempted violations. Nevertheless, while difficult to quantify, the potential harm of even isolated incidents (e.g., discriminatory items or privacy-invasive products) may be significant in terms of scope and scale. However, Whaleco believes that its control effectiveness is high and effective in mitigating the risks. The ratio of user reports and own initiative measures also shows that its moderation measures deal effectively with the inherent systemic risks. A point of attention remains the median response times for notices on Fundamental Rights-related issues during the Relevant Period not exceeding 24 hours. While in line with or better than market standards, this nonetheless leaves potential room for fundamental rights infringements.

Based on the assessment set out above, the overall residual risk for fundamental rights is therefore assessed as "**Low**". While systemic safeguards are strong, the potential impact of even small numbers of incidents prevents a lower categorisation.

Module	Inherent Systemic Risk	Control Strength	Residual Risk
Fundamental Rights	Low-Medium (2/5)	Mostly Effective (4/5)	Low (1/5)

As described above and in line with Article 35(1) of the DSA, Whaleco has put in place reasonable, proportionate and effective mitigation measures to address systemic risks in relation to fundamental rights violations, which include identifying enhancements to these measures. To address the residual risks and potential insufficiencies of the existing mitigation measures identified in the Year 2 risk assessment, Whaleco plans on improving its mitigation measures against fundamental rights infringement risks in the following areas:

Mitigation Type	Description (DSA Article 35)	Controls	Control Enhancement Description
Internal risk management and oversight	Adapting content moderation processes, including the speed and quality of processing notices related to specific types of illegal content and, where appropriate, the expeditious removal of, or the disabling of access to, the content notified, in particular in respect of illegal hate speech or cyber violence, as well as adapting any relevant decision-making processes and dedicated resources for content moderation	Review of decision procedures	Whaleco will explore ways to bring down median response times in relation to data subject requests and appeals against measures taken in respect of users and traders to minimise exposure to potential fundamental rights infringements.
Onboarding and training	Taking awareness-raising measures and adapting their online interface in order to give recipients of services more information.	Seller Portal	Whaleco will review training materials for traders and consider whether to include extra material on fundamental rights and data protection.

X. Conclusion

Whaleco conducted this Year 2 risk assessment with full recognition of the range of inherent systemic risks that can arise in the operation of a cross-border online marketplace such as Temu. As reflected in this Report, those potential risks that Whaleco has assessed are broad in scope, ranging from unsafe and counterfeit products to fraudulent transactions, misleading trader conduct, and adverse impact on users' mental well-being. In response to those risks, Whaleco conducted this assessment pursuant to its Risk Governance Framework, covering 1) governance, risk & compliance oversight (GRC), 2) policies & standards, 3) user management & onboarding control, 4) detection & enforcement, 5) user rights & redress mechanisms, and 6) external engagement.

As this Report demonstrates, during the Relevant Period, Whaleco has introduced improvements to Temu's design and operational processes to address and mitigate such risks. Many of these changes were informed by ongoing engagement with EU regulators and other stakeholders.

In line with the DSA's objectives, Whaleco's risk assessment strategy is not a one-time or occasional exercise, but rather a continuous process. Going forward, Whaleco will continue to monitor the potential evolution of risks as the Temu platform continues to grow and develop, in an effort to evaluate the effectiveness of current mitigations while implementing any necessary adaptations and enhancements to existing mitigation measures. As this process continues, Whaleco also remains committed to open dialogue with EU authorities, consumer groups, rights holders, and users alike. Such efforts will only further Whaleco's ultimate objective of strengthening its approach to systemic risk and ensuring Temu's status as a safe, transparent, and reliable marketplace for EU consumers.