Digital Services Act
Risk Assessment and Mitigation Measures Report
2024

(Non-Confidential version)

Table of Contents

I. Executive Summary

Launched in 2010, AliExpress (hereinafter referred to also as "**we**", the "**Platform**", "**us**" or "**our**") is a business-to-consumer (B2C) e-commerce platform enabling global consumers to buy directly from manufacturers and distributors in China and around the world. AliExpress enables users from over 100 countries and regions to access an extensive range of quality products at competitive prices. From apparel and electronics to jewellery, watches, home goods, furniture, and health & beauty products, the Platform caters to diverse shopping needs. With a vision to empower our customers, our mission underscores a commitment to enabling a life of choice and to promoting 'Smarter Shopping, Better Living'. At AliExpress, we value the safety of our users, and have developed terms and conditions as well as policies, echoing the principles of the EU Charter of Fundamental Rights.

In line with the obligation laid out in the Regulation (EU) 2022/2065 (the Digital Services Act, or "**DSA**"), and following AliExpress' designation by the European Commission as a Very Large Online Platform ("**VLOP**") in 2023 ("**Year 1**"), we conducted our first inaugural systemic risk assessment. This year ("**Year 2**"), we have built on the baseline set in Year 1 and taken a number of steps to enhance our approach in the assessment of risks and effectiveness of our mitigation measures.

In Year 2 we refined our methodology in several areas, including around our assessment of probability and severity to more accurately capture the systemic risks and how they can stem from the design or functioning of our services, algorithmic system or from the use made of our services by sellers and buyers. We have also updated our assessment of mitigation effectiveness based on the Digital Trust and Safety Partnership (DTSP) Safe Assessments Methodology, where an overall mitigation effectiveness score was computed based on the maturity scores assigned to each assessment response.

We conducted this assessment supported by our strong risk governance structures, including the DSA Compliance Function, the Legal & Compliance Department, the Chief Risk Office ("**CRO**"), the Platform Rules Department, the Internal Control Department, our Global IP Enforcement Team, and Emergency Service Unit ("**ESU"**) and consulted with key internal and external stakeholders and subject matter experts.

The current assessment captures the four systemic risk categories outlined in Article 34(1) and analyses them through five separate modules focusing on the risks that are specific to our services: (i) Prohibited and Controlled Products ("**P&C"**), (ii) Intellectual Property Rights ("**IPR**"), (iii) Content Compliance, (iv) Data Protection and (v) Consumer Protection and Related Fundamental Rights.

We assessed a total of two modules with "High" inherent risk rating and none with a "High" residual risk rating after the mitigation effectiveness was considered. Specifically, P&C and Consumer Protection and Related Fundamental Rights modules were assessed to be of "High" inherent risk due to the high severity and high risk probability. For the P&C module, the "High" inherent risk was comparable to the Year 1 Risk Assessment, while for the Consumer Protection and Related Fundamental Rights module, the inherent risk rating in Year 2 was higher than Year 1 due to updates to the risk scoring methodology. For the IPR module, the inherent risk rating was assessed to be

"Medium High" and the residual risk rating was assessed to be "Low Medium", which is similar to Year 1. For the Content Compliance module, the inherent risk rating was assessed to be "Low Medium" and the residual risk rating was assessed to be "Low", which is also similar to Year 1. Lastly, for the Data Protection module, the inherent risk rating was assessed to be "Medium High" and the residual risk rating was assessed to be "Low Medium", which is lower than Year 1. Overall, the reduction in inherent risk profile was due to the robust risk mitigations including progress made on developing new mitigations and improvements to existing mitigation measures in Year 2.

In light of the residual risks identified, we plan to further implement, in the upcoming year, improvements to strengthen our ability to detect, prevent and mitigate these risks. This will include (i) optimising our algorithmic controls, (ii) expanding reactive reporting channels, (iii) increasing penalties for severe violations and repeated offenders, (iv) improving support for users and right-holders and (v) deepening collaboration with external partners. These mitigation strategies will further evolve our existing set of reasonable, proportionate and effective controls that collectively seek to address the dynamic risk landscape in which our services operate.

These efforts continue to contribute to our goal of enabling a safe and secure experience where sellers can offer, and buyers can benefit from, access to a diverse range of products knowing that their safety and privacy is our top priority. We look forward to continuing these annual assessments and welcome feedback on our approach from the Commission, researchers and civil society.

II. Introduction

Building on the foundational work established in the first risk assessment under the European Union ("**EU**") Digital Services Act conducted in 2023 (Year 1), AliExpress hereby summarises the results of its second DSA risk assessment for Year 2, which has been prepared based on data covering the period starting from 1 July 2023 (i.e., the date falling immediately after the end of Year 1 risk assessment) until 30 June 2024 (both inclusive). The time frame ensures a comprehensive coverage of Year 2 and allows for sufficient time for the extraction and analysis of the data in order to conduct this risk assessment. This Report (the "**Report**") reflects AliExpress' commitment to continuous improvement in identifying and mitigating systemic risks stemming from the design or functioning of our services in the EU and to ensure that the Platform remains a safe, trustworthy marketplace for users in the EU.

AliExpress provides an "information society service", as defined under the EU E-Commerce Directive (Directive (EU) 2015/1535). Specifically, in DSA terms, AliExpress operates an online platform that allows consumers to conclude distance contracts with traders. Since its launch in 2010 as a business-to-consumer online marketplace, AliExpress has enabled business sellers and consumers to share product listings, exchange product information, and complete transactions. The seller bears the obligations related to the sales agreements, including storing, delivery and after-sales, while AliExpress provides customer service and support for buyer-seller disputes.

The Year 1 Risk Assessment set a strong baseline for identifying and mitigating the risks stemming from the design or functioning of the Platform. Taking into account new literature, industry best practices and initial regulatory feedback, AliExpress has built on the reflections and learnings from Year 1 to allow for a more nuanced analysis in Year 2. Concretely, the following changes were made between the Year 1 and Year 2:

- **Methodology**: We have updated our methodology for Year 2 by streamlining our assessment of certain sub-categories of related risks. We have refined the risk assessment questionnaires to align more closely with Article 34(2) of the DSA and also enhanced our scoring methodology to allow for a more granular evaluation of systemic risks.
- **Platform Environment**: We have given specific attention to the changes on the Platform between Year 1 and Year 2 and assessed their impacts on the systemic risks, including those stemming from new features or the growing relevance of certain business models.

In conducting this assessment, we have rigorously identified the risks that may materialise through the design or functioning of AliExpress in the EU; analysed the effectiveness of our existing controls; identified potential areas for improvement; and considered targeted mitigation strategies to address residual risks.

As laid out under Article 34(3) of the DSA, the relevant supporting documentation and data used for the assessment have been preserved in a separate internal repository to allow us to monitor the evolution of the risks over time, track the progress of our mitigation measures, and allow for continuous improvements to our methodology over time.

Our Year 2 Risk Assessment not only reinforces our dedication to comply with the DSA but also underscores our proactive approach to navigating the complexities of operating a digital marketplace. As we move forward, AliExpress remains steadfast in our commitment to upholding the highest standards of safety, security, and user trust while protecting their fundamental rights.

III. Consultations with Stakeholders

To meet due diligence requirements, we have sought input and guidance from suitably qualified subject matter experts, including feedback from the European Commission, other national and regional authorities from EU member states, specialised consultants and other stakeholders. We have sought their knowledge and expertise where necessary to comprehensively assess the systemic risks stemming from the design and functioning of our services and get their insights around any emergent areas of concern, allowing us to refine our approach to stay ahead of potential future risks.

The Year 2 systemic risk assessment exercise has also involved a number of AliExpress internal teams, including representatives from CRO, Legal & Compliance, Government Affairs, Internal Control, Product Design, Tech, Finance, Marketing, Europe Country Business, Global IP Enforcement, and the Customer Service teams among others. This has enabled us to conduct the assessment based on the most accurate, comprehensive and up-to-date information across the entire company. Given the importance of this exercise, the business group in which AliExpress is integrated, Alibaba International Digital Commerce (AIDC), also contributed resources and insights from its Legal & Compliance and CRO functions.

To enhance our risk management and compliance capabilities further, we regularly invite external agencies, such as the British Standards Institution (BSI), to annually audit key certifications, including ISO 27001/27701 for information security and privacy management and PCI-DSS for payment security, demonstrating our commitment to adhere to privacy protection laws, regulatory standards and best practices.

In addition to these certifications, we partner with leading compliance service providers to enhance our detection, prevention and enforcement strategies across high-risk areas for content and products on the Platform. These collaborations enable us to leverage expert insights and advanced tools to monitor external channels, conduct analyses of product listings, identify trends in fraudulent behaviour, and monitor merchant activities across various markets, to further strengthen the Platform's defences against fraud and unauthorised activities.

IV. Risk Governance Framework

To comply with Article 41(1) of the DSA, following AliExpress' designation as a VLOP, the European Legal & Compliance team and the European Risk Management team focus on the European region under the coordination of the DSA Compliance Function established in compliance with the DSA.

There are specialist teams within the Legal & Compliance team and/or the Chief Risk Office who are each responsible for a specific function (e.g., Prohibited & Restricted, IPR, etc.), this specialised functional team will take the lead in addressing concerns that may arise in these areas, while the European Legal Team and/or the European CRO team remain involved in issues that pertain to or impacts EU DSA compliance. In cases where there is no dedicated functional team and the matter relates to DSA compliance or impacts DSA compliance, the European Legal Team and/or European CRO team take the lead, involving other teams as appropriate under the coordination of the DSA Compliance Function.

The European Legal Team and the European CRO team are at the heart of the DSA Task Force, jointly leading the implementation of AliExpress's DSA compliance efforts and continuing to provide support in collaboration with other functional teams from Legal & Compliance, CRO, or other areas (e.g., the Platform rule department, Product Design, Tech, etc.).

Specifically, to ensure the Platform remains compliant with the DSA's requirements, the European Legal Team and the European CRO Team will regularly monitor and prepare periodic DSA Compliance Reports under the coordination of the DSA Compliance Function. The reports will be sent and/or presented to AliExpress management body by the Head of the AliExpress Compliance Function in meetings, covering relevant DSA compliance matters (e.g., activities related to independent audits, risk mitigation measures, risk strategies and policies, risk assessment plans, compliance data monitoring, etc.).

An overview of the core functions involved in DSA compliance matters is provided below:

- **The DSA Compliance Function** is independent from the Platform's operational functions and holds the necessary authority and resources to both investigate and address compliance concerns. The contact details of the Head of the Compliance Function were also informally communicated in 2023 to the ACM, which this year was subsequently designated by the Netherlands as its Digital Services Coordinator. In January 2024, AliExpress International (Netherlands) B.V. ("**AliExpress Netherlands**") took over from Alibaba (Netherlands) B.V. as our EU establishment for DSA purposes, i.e., the Platform's EU establishment remains based in the Netherlands. This change was communicated in a timely manner to the European Commission and the ACM.
- **The Legal & Compliance Department** monitors legal requirements globally, identifies shifts in regulations, and converts legal provisions into guidelines that can be effectively implemented on the Platform. The **Europe Legal & Compliance** team focuses on the European region, including DSA matters.

- **The CRO** verifies that products meet the required standards and certifications, oversees the content compliance adherence, and ensures regulatory compliance through relevant tools and processes. Within the CRO, the **Europe Risk Management** team (under the Business Risk Management department) is the core team responsible for DSA compliance. The CRO creates and enforces standardised operating procedures ("**SOPs**") for reviewing products, conducts manual and automated assessments, and takes action against violating products. We provide avenues for appeals and user reports, with dedicated teams tasked with verifying and responding to such cases. Regarding the DSA systemic risk assessment process, the DSA Compliance Function, with the support of the Europe Legal & Compliance and the Europe Risk Management teams, evaluates the risk assessment modules, mitigation plans, and the implementation of mitigations. The DSA Compliance Function reports periodically to the Board of Alibaba.com Singapore E-commerce Private Limited (i.e., AliExpress service provider, but also to the board of our EU establishment, AliExpress Netherlands), who oversees the overall implementation of AliExpress' DSA commitments.
- **The Platform Rules Department** formulates and enforces platform rules and policies governing sellers' product listings, information dissemination, and seller education, integrating insights from legal interpretations and understanding the unique characteristics of e-commerce. The team also designs punitive measures for violations, encompassing actions such as content removal, point deductions, and permission restrictions.
- **The Internal Control Department** provides internal inspection and control support regarding the procedures and tools in place to comply with different legal requirements and company policies.
- **Crisis Management**: AliExpress operates a special cross-departmental Emergency Service Unit (ESU) to standardise the management of public emergencies, improve the ability to deal with public incidents and formulate a scientific, effective and responsive emergency service mechanism. The members of this unit include CRO, Customer Chief Office (CCO), Legal & Compliance, Public Relations and technology representatives. We have a robust crisis control process in place to classify risk types within technical security, data compliance, commodity safety, loss of funds, regulatory directives and public opinion, and also to classify risk levels from E4 to E1 with corresponding step-by-step alarm and treatment measures.

V. Risk Assessment Methodology

The Year 2 Risk Assessment exercise, as summarised in this Report, reflects the risk profile of our services as of 30 June 2024. In compliance with Article 34 DSA, AliExpress' systemic risk assessment methodology evaluates how the Platform may contribute to systemic risks in the EU, as outlined in Article 34(1). The assessment has taken into account the relevant recitals of the DSA, i.e., 12, 79, 80, 81, 82, 83, 84, 85, 89, and 90 and covers the four categories of systemic risks, notably:

1. the dissemination of illegal content through our services;
2. any actual and foreseeable negative effects to the exercise of fundamental rights;
3. any actual or foreseeable negative effects in relation to civic discourse, electoral processes, public security; and,
4. any actual or foreseeable negative effects in relation to gender-based violence, the protection of public health and minors and serious negative consequences to the person's physical and mental well-being.

As part of our ongoing risk management efforts, we have refined and streamlined our Year 1 methodology in Year 2, drawing our updates from new literature and industry best practices (including considerations made in the DTSP Safe Assessments Methodology [1] and the EUCRA Report [2]). Specifically, we have updated our risk register to streamline our analysis and more closely align with the specific systemic risks that can materialise from the design or functioning of AliExpress as per Article 34(1). Additionally, we have redesigned the risk assessment questionnaires to align more closely with Article 34(2) of the DSA in order to conduct a more comprehensive analysis of the key features and related systems in the Platform that may influence the systemic risks. Finally, we also enhanced our risk scoring methodology to allow for a more granular evaluation of the inherent risks, mitigation effectiveness and the residual risk scores, with the aim to more accurately reflect the extent of risks and AliExpress' control measures on the Platform.

Similar to Year 1, we have followed a four-phase approach to identify, analyse, and assess any systemic risk stemming from the design or functioning of AliExpress and its related systems, including algorithmic systems, or from the usage of our services. *Figure 1* provides an overview of the assessment methodology, with detailed updates for the 4 phases in Year 2 Risk Assessment Process outlined below:

[1] More information can be found at: https://dtspartnership.org/wp-content/uploads/2022/07/DTSP_Report_Safe_Assessments.pdf
[2] More information can be found at: https://www.eea.europa.eu/publications/european-climate-risk-assessment

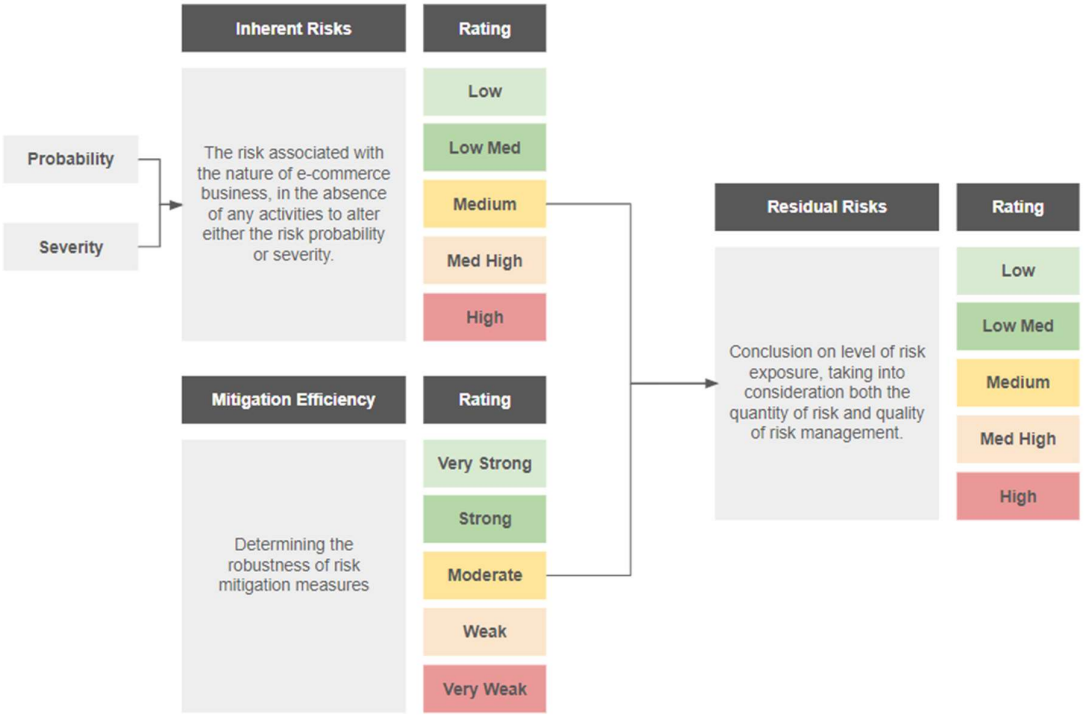

Figure 1: Overview of the risk assessment methodology

Phase I: Identification of Systemic Risks

In Year 2, we maintained the five risk modules based on the four systemic risk categories outlined in Article 34(1), but with some changes to the classification of certain risk sub-categories within certain modules.

To streamline the assessment process, we have adopted a more holistic approach by evaluating related sub-categories of systemic risks together. This aligns our methodology more closely with the requirements of Article 34(1) of the DSA, which mandates that risk assessments be specific to the service. By doing so, we (i) ensure consistency with the Transparency Reporting Statement of Reason (SoR) categories; (ii) better capture the intended use of AliExpress as an online marketplace; and (iii) address the specific risks associated with the functioning of such a service. Table 1 summarises the updated risk registry used for the Year 2 Risk Assessment.

Risk Modules	Year 2 Risk Sub-Categories
Prohibited & Controlled Products	Public security (dangerous products)
	Sale of non-compliant products
Content Compliance	Illegal hate speech

	Unlawful discriminatory content
	Terrorist content
	Public Security (mass violence)
	Child Sexual Abuse Material
	Gender Based Violence
	Non-consensual sharing of private images
Data Protection	Protection of personal data
Consumer Protection and Related Fundamental Rights	Online stalking
	Rights of the child & Protection of Minors
	Online interface design that may stimulate behavioural addictions of recipients of the service
	Right to effective remedy and to fair trial
	Risk to public health (Previously called coordinated disinformation campaign related to public health)
	Sale of products or provisions of services in infringement of consumer protection law
	Freedom of expression and information
	Freedom to conduct a business
Intellectual Property Rights (IPR)	IPR infringement (including patent, trademark and copyright) (Previously called Non-authorised use of copyright protected material)

Table 1: Updated risk registry for Year 2 Risk Assessment

Phase II: Assessing Inherent Risks

Similar to Year 1, the inherent risks assessment involved analysing the risks arising from the features, design, functionality of the Platform and its related systems (including algorithmic systems) in a hypothetical scenario, as if there were no controls in place. We have updated the risk assessment questionnaires for each of the five risk modules, which allows for a more consistent, in depth, and systematic assessment of the key features outlined in Article 34(2), including the design of the recommender system, the content moderation systems, applicable terms and conditions and their enforcement, advertisement systems and data related practices. The assessment also considers how the identified risks were influenced by inauthentic and misuse of our services, along with the specific regional or linguistic aspects of the different EU member states.

As defined in Article 34(1), the **inherent risk level** takes into consideration (1) the **probability of the risk** occurring, and (2) the **severity of the risk**.

Probability

The probability of risk occurring is calculated by taking into consideration (i) the number of times a particular type of risk occurred over the assessed period and (ii) comparing it to the weight it represents on the total volume of a specific category of business operations run on AliExpress within a given statistical cycle. As much as possible, we have aligned the probability calculation with the metrics published in our transparency reports to ensure consistency. The data period is therefore from 1 July 2023 to 30 June 2024 to align the transparency reporting with the Risk Assessment.[3]

As no data can truly measure the probability of a risk occurring without controls in place, given that this is a hypothetical scenario we used the closest proxy we have to estimate the potential probability of the risk materialising on our services. In Year 2, we have used the same probability thresholds as in Year 1 to maintain consistency and comparability[4].

Severity

In Year 2, we enhanced our approach to assessing the potential severity of the inherent risks to align more closely with emerging best practices in the space by updating our questionnaires, and supporting them with data quantifications. The severity questionnaire was developed based on the UN Guiding Principles on Business and Human Rights framework[5], which highlights the following characteristics as impacting the severity of the risks:

1. Scope (the number of individuals that are or could be affected);
2. Scale (gravity of the impact on the human right(s)) and

[3] Please note that, for technical reasons, in some situations the data may not be available for the full period, in which case, we have brought in what data we have available, and highlighted the time period it covers.

[4] See **Annex 1** for more details on the scoring.

[5] More information can be found at:
https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf

3. Remediability (the ease with which those impacted could be restored to their prior enjoyment of the right(s)).

For each risk module, an overall severity score was computed based on the holistic assessment of the three severity characteristics above. Scores range from 1 (Very Low) to 5 (Very High), and reflect the potential impact of the identified risks, considering both the extent and range of harm as well as the ease of recovery (**Annex 2** for more details on the scoring).

Inherent Risk Score

Similar to Year 1, the **inherent risk score** was derived by plotting the probability of occurrence and potential severity of impact on users in a matrix[6]. The inherent risk scores[7] range from "High," indicating a high likelihood of occurrence with significant negative consequences, to "Low," where the occurrence is very rare and the impact is minimal.

Note: The purpose of this approach is to enable readers to evaluate and comprehend the risks in terms that are more concrete and accessible. These assessments are constructed from a combination of quantitative and qualitative evaluations, and it is essential that they be interpreted within this context. Nevertheless, we are confident that these assessments serve as a meaningful illustration of the relevant risks, providing a well-rounded perspective that reflects both numerical analysis and nuanced understanding.

Phase III: Assessing Mitigation Measures Effectiveness

After assessing the inherent risks, the next step involved measuring the effectiveness of the existing mitigating measures. In Year 2, the overall mitigation effectiveness score was updated to a 5-scale scoring (from a 3-scale scoring in Year 1) to provide greater granularity and better reflect the effectiveness of the mitigation measures implemented. A structured questionnaire was created to determine the maturity levels of each mitigation measure based on industry best practices in line with the DTSP Safe Assessments Methodology, which is among the most developed and recognised in the online trust and safety industry. An overall mitigation effectiveness score was computed based on the maturity scores assigned to each assessment response.

Phase IV: Assessing and Addressing Residual Risks

After assessing both the inherent risks associated with our services and the effectiveness of the existing risk mitigation measures, we mapped the inherent risk scores to the mitigation effectiveness scores[8] to obtain the residual risk score[9] for each of the five risk modules. This process enabled us to

[6] See **Annex 3** for more details on the scoring.
[7] See **Annex 3** for more details on the scoring.
[8] See **Annex 4** for more details on the scoring.
[9] See **Annex 5** for more details on the scoring.

evaluate the remaining level of concern regarding the likelihood and impact of risks to users on the Platform after mitigations have been applied.

However, despite our best efforts, certain risks stemming from the designing and functioning of our services may remain. In fact, a level of residual risks is inevitable given that the nature of the risks faced are in constant evolution. In response to this, a continuous risk-based monitoring and enforcement mechanism has been implemented in place to identify and respond to these evolving risks on AliExpress.

Similar to Year 1, in accordance with Article 35 of the DSA, we considered where existing mitigation measures could be adjusted and where additional measures could be implemented to further reduce residual risks and respond to the emerging risks related to our user community or business developments. In Year 2 we have incorporated our discussion of residual risk mitigation roadmap within each of the risk modules for greater coherence with our risk assessment and alignment with Article 35(1) of the DSA. For example, we have mapped our mitigation roadmap with the 11 categories of mitigation measures under Article 35(1), where applicable.

VI. Summary of the Platform Environment

Systemic risks on AliExpress can be best understood by examining the core components of the Platform's environment. As an online marketplace, AliExpress primarily facilitates transactions between buyers and sellers. Therefore, certain elements, such as the increase in user numbers, the expansion of local sellers and their product assortments to cover more EU countries, and the growing complexity of our services contribute to a dynamic platform landscape. As AliExpress continues to gain popularity, it may unfortunately attract "bad actors", or fraudulent buyers or sellers who may innovate new product control and content moderation evasion tactics, further complicating our risk environment.

The factors highlighted in Article 34(2) of the DSA are integral to the Platform's overall functioning and frequently reappear across various risk assessment modules. Additionally, we have included elements and features outside of Article 34(2) that we believe are important to explain in order to provide a more comprehensive understanding of the Platform environment. These include:

- **Platform design and functionalities:** As an online marketplace, the main risk vector on AliExpress is linked to the ability to post product listings that allow buyers and sellers to conclude distance contracts. Some listings may contain illegal or controlled products (analysed in the Prohibited & Controlled Products, "**P&C**", Module) or IPR-infringing goods (IPR Module). Other Platform functionalities may also contribute to systemic risks. For instance, instant messaging ("**IM**") may be misused to discuss the sale of prohibited and controlled items ("**P&C**") or IPR-infringing goods. Users may also use IM, comments or reviews to share violating content, such as discriminatory or hateful language (see Content Compliance Module). Similarly, delivering an ordered product requires giving sellers some level of access to buyers' data which, in the absence of any controls, may lead to data protection risks (see Data Protection Module).
- **Inauthentic use:** The Platform additionally faces risks related to inauthentic use of the Platform's functionalities. These actions can undermine the trustworthiness of the marketplace, mislead genuine buyers, and distort the perceived quality or legitimacy of products, leading to systemic risks for the Platform's integrity and user experience.
- **Advertising systems**: The only type of users that can place advertisements on AliExpress are sellers, which may choose to place ads in search and/or recommendation scenarios. By setting factors such as the delivery country and application bid, the recommender system uses inferred parameters (such as previous shopping history or interests, age, gender, purchasing amounts, etc.) to facilitate more accurate matching between sellers and potential buyers. Based on the AliExpress's advertising bidding mechanism and the profiling techniques of the recommender system, sellers can pay a premium to obtain greater probability of reaching specific groups of people. Before purchasing advertising services, sellers agree to our advertising policies. Additionally, the showing of adverts occurs downstream from product control at the product listing and display stage, therefore any product that has been blocked from publication cannot be advertised. The Platform also applies proactive controls to detect non-compliant ads before they are displayed. However, there remains a risk that illegal

products (P&C and IPR) may be shared on the Platform (whether as advertisements or otherwise).

- **Recommender system:** We use a single recommender system across the entire Platform with different product ranking logics for the different scenarios where information is displayed. As indicated in AliExpress' Terms and Conditions, the main parameters used for recommendations are inferred from the user's profile: location, search history, shopping behaviour and member profile information (such as age, city, interests, purchased amount). Additionally, the recommendation pool is directly connected to the database of sensitive product content (such as Halloween-related horror elements that are not suitable for proactive recommendations), therefore any products with content found in that database will be automatically excluded from the recommendation pool, in order to safeguard users' experiences with the recommendation system on the Platform.
- **Data and content moderation systems:** AliExpress' systems span technology, people, and processes. Content moderation on the Platform is managed through the internal risk management system ("**MTEE**"). MTEE provides the backbone for our proactive detection algorithms (text-based, image-based and combined indicators) and manual review and audit teams (including the CRO, specialised product teams, and trained moderation staff).
- **Applicable policies:** We have a wide range of policies that users agree to when joining the Platform, which guide manual and automated enforcement. Our policies are necessarily dynamic, adapting to new risk vectors and emerging regulations.
- **Regional and linguistic diversity:** 99% of product-related content on the Platform is published in English. Non-English language content by sellers is automatically translated to English for algorithmic identification, while non-text-based systems are capable of identifying problematic listings regardless of language.
- **Choice service:** during this year our "Choice" service has gained in popularity, in which AliExpress provides additional supply chain and other value-added services to sellers, shortening the supply chain so it can offer better value for money to buyers and simplified operations for sellers. While the exact scope of "Choice" is still under experimentation, it basically involves certain operational aspects, such as customer acquisition, product listing, logistics or after-sales services.
- **Affiliate program:** AliExpress users with a buyer account can apply to become a participant of the Affiliate Program in order to derive commission revenue from the promotion of products outside AliExpress as an affiliate.
- **Off-Platform risks:** In light of the success of our internal moderation tools, certain sellers have attempted to bypass controls by resorting to off-platform means, such as using hidden links, which originate on social media sites, standalone websites, chat applications, and search engines.

VII. Prohibited and Controlled Products

I. Risk Definition

In the Prohibited and Controlled module, we analysed the risk(s) that the design or functioning of the Platform and its related systems (including algorithmics systems) may be used to disseminate, or contribute to disseminating P&C products. Prohibited products refer to items that are not allowed to be listed and sold on the marketplace as stipulated by a governing body within its jurisdiction. Meanwhile, controlled products refer to items that are restricted and should meet relevant qualification requirements due to safety concerns or are subject to controlled selling or posting regulations, or other requirements, in accordance with the laws of relevant jurisdictions. For example, an item may need to meet special requirements such as producer licensing, labelling standards, or product certifications (as the case may be) in order to be listed and sold on the marketplace.

In this regard, our assessment of this module takes reference from applicable EU laws, including the recently passed Regulation 2023/988 on general product safety, and focuses on the risk of disseminating illegal products, as outlined in Article 34(1)(a) of the DSA, including:

- The sale of non-compliant products.
- The dissemination of dangerous products that pose a threat to public security.

In certain cases, the sale of products on the Platform could result in negative effects to Fundamental Rights laid down in the Charter of Fundamental Rights of the European Union (2000/C364/1) ("**the EU Charter**"). For example, certain products may infringe on the integrity of the person. As the risk of negative effects to fundamental rights arises from the risk of dissemination of prohibited products, controls that apply to curbing P&C products being sold also serve to mitigate such risks to fundamental rights. As such, we have assessed those relevant fundamental rights as part of the overall P&C products module.

II. Inherent Risk

Given the dynamic nature of the risk and the high volume of sellers attempting to list prohibited and non-compliant controlled products, AliExpress has conducted a more in-depth analysis in Year 2, building upon the baseline of the risks identified in Year 1. This analysis focuses on how various Platform features and factors, including those outlined in Article 34(2)(a) of the DSA, contribute to this risk.

a. Risks from Platform Design and Functionalities, including their misuse

AliExpress acts as a marketplace to facilitate transactions between sellers and buyers on the Platform. The most common functionality used by sellers which may create or contribute to the risk of the dissemination of P&C products on the Platform is to attempt to publish, list and sell P&C items. The functionalities of publishing products include uploading and publishing text, photo and video content

in the form of full product listings, product pictures and videos, product titles and descriptions as well as reviews and hyperlinks that may enable off-Platform purchasing behaviour. Often, the illegal information will be included in either the title of the product, main pictures or videos, product specification (brand, certification, model number, etc.) and product description (text or pictures).

Sellers may also misuse the Platform functionalities to publish and sell P&C products through the following ways:

- **Misrepresentation of product details:** [*Confidential*].
- **Falsification of qualification documents:** Sellers in categories requiring compliance qualifications must upload documentation such as product compliance certificates, test reports and/or product packaging label pictures when listing controlled products. [*Confidential*].
- **Misplaced product categories:** We have strict category governance controls for certain product categories that require specific qualifications as mentioned above. [*Confidential*].

In addition to functionalities which allow users to list and publish products, there are other functions that may be used to distribute P&C products that have been published on AliExpress (such as IM, Buyer Question & Answers, Order Details, Feed - a stream of content that you can scroll through with short video - Livestream, Reviews and the Affiliate Program). As these functionalities are closely linked to the risk of disseminating illegal content (e.g., hate speech, pornography, violent content etc.) on the Platform, details about these functionalities are discussed more comprehensively in the Content Compliance and IPR modules.

The sale and purchase of P&C products on the Platform can result in potentially significant harm, including physical injury, psychological distress, and financial loss for those affected. This is a serious concern for all users.

However, there is an additional risk related to minors. Although AliExpress is intended solely for adult use, minors might still access the Platform [*Confidential – bypassing the mechanisms of control*]. This exposes them to products that are inappropriate or unsafe for their age, potentially leading to further harm.

In Year 2, we identified that the expansion of the AliExpress services to sellers from additional EU countries (e.g., in Poland and Germany) may theoretically contribute to the increased risk of disseminating P&C products on the Platform in general, as would every expansion of services to new regions. However, considering that sellers from the EU are more likely to offer products that are already compliant with local regulations, the expansion of a more likely compliant product pool could, in fact, reduce the likelihood of P&C products reaching EU consumers.

b. Risks from Other Factors of the Platform (in line with Article 34(2) of the DSA)

Both in Year 1 and Year 2, we have assessed how the factors listed in Article 34(2) of the DSA may influence the risks of disseminating P&C products. Please refer to Section VI for more context on these factors.

- **Advertising systems and data practices:** There is a risk that sellers manage to successfully publish P&C products on AliExpress and advertise them on the Platform if our product compliance controls or advertising controls do not detect and remove the products before they are being advertised. While it is not possible to assess the full scale of this risk, the historical volume of detected infringements can serve as a proxy for this particular risk. Among the products removed by the Platform due to violations of P&C product rules in the time period from 1 July 2023 to 30 June 2024, 6% of them ([*Confidential*]) were advertised.
- **Recommender system***:* If sellers manage to evade our proactive product compliance controls and publish their P&C products, there is a risk that such products may be recommended to users through our recommender system. While it is not possible to assess the full scale of this risk, the historical volume of detected infringements can serve as a proxy for this particular risk. Among the products removed by the Platform due to violations of P&C product rules in the time period from 1 July 2023 to 30 June 2024, a total of 14,746,471 P&C products were recommended by our recommender system in the EU.
- **Relevant policies:** As legislation gets updated in various countries, our P&C Product Listing Policy and related platform rules could become outdated and would need to be continuously iterated upon. Inaccurate policy enforcement (such as due to technology system failure and human errors) could also contribute to this risk. While it is not possible to assess the full scale of this risk, the number of P&C product policies and guidelines that have been updated can serve as a proxy for this particular risk. Between 1 July 2023 and 30 June 2024, 274 policies and guidelines around P&C products were updated to ensure applicability.
- **Content moderation systems and product compliance controls:** Our content moderation systems and product compliance controls are designed to reduce risks of disseminating P&C products. However, certain P&C products could fail to be identified by either algorithmic detection systems (e.g., new and evolving risks that the algorithms have not been sufficiently trained on, detection system failures and downtime) or be missed by the human reviewers. The review process could also not be able to deal with the identified illegal products quickly enough. While it is not possible to assess the full scale of this risk, the historical volume of P&C products that were blocked due to reactive reports can serve as a proxy for this particular risk. Between 1 July 2023 to 30 June 2024, a total of 10,737 P&C products were blocked due to reactive reports. This figure represents 0.05% of all P&C products removed from the Platform worldwide during the same period.

Given that AliExpress operates as a marketplace, the potential theoretical risk—assuming no controls are in place—of dissemination of P&C products is “High”. While it is not possible to measure the risk without any controls in place, this risk can be estimated by examining the number of products that were blocked or removed based on P&C product rules, and the number of sellers that were removed for violating rules for P&C products. Between 1 July 2023 and 30 June 2024, 1,148,061 P&C items were removed in the EU and 11,659 sellers were blocked for non-compliance with AliExpress’ rules on P&C products. Further, we can also infer that there are not only sellers that are motivated to attempt to sell P&C products, but also buyers that are looking to purchase them. This is evident from the blocking

of prohibited search terms, which occurred 15,591,798 times worldwide between 27 March 2024 and 30 June 2024 [*Confidential*].

III. Existing Mitigations

In Year 2, we continued to operate strong control mechanisms and further enhanced our P&C Product controls through our Year 1 mitigation commitments and adapting them to address specific events that could act as P&C product risk vectors in the EU.

a. Algorithmic Controls

We operate a comprehensive and sophisticated risk identification system to proactively detect the majority of violating P&C products before they get published. Meanwhile, we continuously optimise and upgrade our system capabilities. The risk identification systems leverage artificial intelligence technology to continuously enhance the detection of illegal products and content on the Platform. Different algorithmic controls are deployed to analyse text, images and videos uploaded by users to detect and block P&C products before they get published. The data collected from the product listings are screened by our automated systems, which continuously screen listing text and images, using our own self-developed detection techniques, to determine whether listed products comply with AliExpress' product compliance rules. Listings identified by the risk identification system as requiring review will be forwarded to a dedicated audit team for further manual review. Product listings found to be in violation are removed and the sellers will be penalised in accordance with the rules stipulated by our violation penalty points system.

On the Platform, there are features to mitigate the risks of P&C products such as the following:

- **Consumer safety warning***:* For those product categories that we identified with potential safety risks, but do not manifestly violate our policies, we have the corresponding consumer safety warning on the product detail page so that buyers are made aware of the safety guidance and the potential risks, notwithstanding sellers' obligations in this regard.
- **Product certification verification***:* the Platform's product listing system includes a certificate upload feature that allows sellers to upload necessary documentation to prove a product's reliability and compliance. For certain high-risk product categories, sellers are required to provide these certificates to meet local compliance standards before listing their products.

The covered product scope for these features has been continuously expanding.

b. Internal Risk Identification

There are several teams and external vendors working together to implement and improve the identification of P&C Product risks. This includes the monitoring of relevant EU and international laws and regulations to inform the formulation of detailed rules that can be implemented by the Platform. Specifically, this entails the development of specific policies for sellers' product listings in various

categories, providing sellers information about P&C products, conducting seller education and awareness on policies and establishing certain account restrictions.

Additionally, there are teams responsible for conducting comprehensive management and control of P&C items on the Platform, including but not limited to the verification of product qualification information and the review of product content. If the product does not meet the policy requirements, the product will be deleted and the seller's store will be penalised, which may even involve the closure of such a store. There is also a team dedicated to investigating and taking action against P&C items reported by users and detected by AliExpress' own monitoring of the relevant regulators' product recall websites. Affected buyers are supported by AliExpress' product recall process and given financial compensation. Between 1 July 2023 and 30 June 2024, around 510,435 products were removed and recalled and 123,769 sellers were enforced.

In addition to product-level checks, there are also account-level verifications. Sellers are required to undergo verification to review their qualifications as a trader and funding account information. This process typically requires sellers to submit business details and licence information, Ultimate Beneficial Owner and legal representative information, and corporate structure information. Only sellers who have passed the verification process are permitted to open a store, which is also helpful to improve the traceability for all products.

In line with DSA Article 20, we provide appeal and service consultation channels for all restrictions of the services, and a dedicated team is responsible for verifying and processing the appeals or answering questions through the consultation channel. Between 1 July 2023 and 30 June 2024, we received 62,221 appeals from 20,519,191 products regarding the Platform's enforcement actions related to P&C product risks. Of these appeals, 5,614 were successful. (i.e., enforcement was overturned).

c. External Risk Identification

AliExpress provides various external reporting channels to complement the internal identification of P&C product risks. The reporting function of the Platform is provided to multiple types of users, such as sellers, buyers and Trusted Flaggers (In line with Art. 22(1) of the DSA). Users will be provided with an acknowledgement of their reports, and once the decisions are made by the Platform (which are all manually reviewed) users will be informed of the decision. Between 1 July 2023 to 30 June 2024, out of all P&C products removed on the Platform, 0.05% of them (10,737 products) were blocked due to reports received from the reporting function of the Platform.

At the same time, the Platform has a designated mailbox (eu.productsafety@aliexpress.com) to receive reports or orders from competent market surveillance authorities in the EU. Dedicated personnel have been charged with promptly handling these complaints from these authorities. After receiving an illegal content report or order from an authority, the illegal products will be taken down and relevant notifications will be sent to the seller to recall the products when applicable. Meanwhile, any information about the illegal product will be added to our proactive monitoring system if they are not already included. Between 1 July 2023 to 30 June 2024, we took down 4,733 illegal products directly reported by EU market surveillance authorities.

We also work with external professional service providers to carry out regular monitoring and manual sampling reviews of the Platform's product listings targeting EU and other markets across multiple languages in high risk product categories to look for suspected illegal listings. These vendors provide regular reports to us to identify latest illegal product risk trends to support our enforcement against illegal products on the Platform and enhance our corresponding proactive product compliance controls. Between 1 July 2023 to 30 June 2024, our external professional service providers sent a total of 25,243 listings to AliExpress by means of the periodic reporting indicated above. Of these listings, 5,881 were EU-related and were either removed or had their accessibility restricted to EU users.

To further improve the detection of unsafe products on the Platform, AliExpress, as an original signatory to the first Product Safety Pledge (in 2018), signed the revamped Product Safety Pledge+ in March 2023. As a signatory to this Pledge, we undertake voluntary commitments going beyond what is already established in EU legislation, including those requirements applicable on product safety.

d. Policies and Enforcement

As introduced in our Year 1 report, we have a number of detailed policies and rules regarding P&C products. To ensure that these policies remain updated and in view of new regulatory requirements, we updated the AliExpress Index of P&C Items in July 2023 and published the AliExpress Compliance Notice on the EU General Product Safety Regulation ("**GPSR**") in June 2024. In addition to specific rules for relevant product categories, the Platform-wide rules for P&C products include (but are not limited to):

- Product Listing Policy.
- Index of P&C Items.
- AliExpress Compliance Notice on the EU GPSR.

Violations of the Platform policies result in the accumulation of penalty points, which are assigned based on the severity of the violation. Penalties against accounts are enforced once these points reach a certain threshold, which depends on the degree of danger or severity of harm involved. General violations add a strike to a seller's account, while extreme violations can trigger account removal with a single strike. This 1-strike policy serves as a deterrent against inauthentic use by users who are malicious or intent on causing significant damage to the Platform.

To enhance policy compliance, we also conduct external compliance training for sellers (such as through the Seller Centre, Message Notification or Offline Events like the Seller Summit). Through our education efforts, we continue to provide product compliance information and knowledge, enhance sellers' product compliance awareness, and seek to reduce their violations and thereby the risks of illegal products on the Platform. For instance, more than 12,000 sellers attended our recent online training for GPSR compliance in August 2024. The training recording also reached 24,000 views as of 30 Aug 2024.

e. Minors Protection

As stipulated in our Terms and Conditions, we do not provide services to minors (individuals under the age of 18), and have specific restrictions on account registration and the use of payment methods. When users register for an account, they are clearly reminded that they must be 18 years or older. Additionally, the requirement for valid payment methods acts as a further control mechanism. More information is included in the Consumer Protection module on this topic.

f. New Mitigation Measures

In line with Year 1 commitments, we have, in the past twelve months, made significant improvements to the effectiveness of our mitigation measures. Notably:

- **Choice service controls:** Choice products have stricter controls than normal products because of the curation of Choice sellers and the screening of products by dedicated AliExpress business teams. After pre-screening and filtering of sellers and products, Choice products generally have lower P&C product risks (along with IPR and non-compliant content risks).
- **Choice service product inspections:** In addition, under the "Full-Entrustment" model of the Choice service, most products will need to be placed into an AliExpress-designated warehouse and will be manually inspected. If a product is detected to have issues (such as P&C or IPR related risks), the Platform will arrange to remove the products from the warehouse or charge for rectification in the warehouse (e.g., adding compliance labels). The full cost of withdrawal will be borne by the sellers, which is intended to deter them from trying to sell non-compliant products in the future. Sellers can also be removed for serious product and transaction-related violations such as the sale of illegal medicines or drugs.
- **Enhanced collaboration with professional service providers:** We have enhanced the scope of cooperation with professional third-party service providers to leverage their specialised expertise in identifying and defining P&C products in specific risk areas. These providers supply text and image samples for risk identification, which are then manually reviewed by our staff, and help detect illegal products for appropriate action.
- **Improved our P&C products violation detection algorithms***:* We have continuously improved our P&C products violation detection algorithms by incorporating a multimodal classification algorithm, which utilises text and image data to enhance detection capabilities. In September 2023, we updated the Image-to-Image algorithm by enhancing capabilities for similar and identical product search to increase product control effectiveness. Strengthened algorithmic product risk controls will help reduce the number of P&C products entering the advertising and recommender product pools downstream, thereby mitigating the risk of disseminating prohibited and controlled products through AliExpress' advertising and recommender systems. More details about risk controls for AliExpress' advertising and recommender systems are included in Section XI on Consumer Protection and Related Fundamental Rights.
- **Enhanced recall process**: We voluntarily identify and recall P&C products to mitigate P&C risks. Additionally, since September 2023, AliExpress has enhanced the recall process for illegal products to actively improve support to users who had purchased these products. Specifically,

we have expanded the scope of the recalled products to include recalls demanded by concerned producers and by local regulators. For certain high risk products, users can receive product recall notice through multiple channels, including email, APP push, APP Message Centre and information published on the AliExpress Recall website, and directly initiate the option of "refund only" without having to return the product, which makes the procedure easier for users.

- **Restrictions on repeat violators**: We have also introduced more severe restrictions for sellers who have repeated violations, such as by raising the penalty points imposed for each violation or by imposing penalty points for infractions that were previously not punished by penalty points.

IV. Residual Risk

Despite our best efforts in mitigating the risk of P&C products on the Platform through proactive and reactive measures, we cannot fully eliminate the risks entirely due to the dynamic nature of the risk landscape, where new illegal products may arise and malicious sellers and buyers may be motivated to transact illegal products. Our efforts to mitigate risk are made more complex by the number of new products regularly added, our global user base, and sellers' attempts to circumvent our controls. Consequently, it is evident that a certain level of residual risks persists on the Platform. Based on the inherent risk score and mitigation effectiveness score of this risk module, the residual risk score is qualified as “Medium” which is comparable to Year 1. Nonetheless, we strive to continue working towards minimising the risk of disseminating P&C products through the Platform.

Inherent Risk	**Mitigation Effectiveness Score**	**Residual Risks**
Based on the probability and severity scores calculated using the DSA Risk Assessment Rating Methodology, the inherent risk score is assessed as “**High**”, which indicates that the probability of the occurrence of risks is high, and they have the potential to have a significant negative impact on users.	Overall, the mitigation implementations are effective and resulted in a decreased exposure of non-compliant products on the Platform. The mitigation effectiveness score is calculated to be “**Strong**” (78%), which indicates minimal likelihood of a control failure.	Based on the inherent risk score and mitigation effectiveness score, the residual risk remains “**Medium**” on the Platform, which indicates a moderate level of concern around the likelihood or impact of risks arising to users on the Platform after mitigation measures have been applied.

V. Conclusion and Future Mitigations

In Year 2, the residual risks rating of “Medium” has remained unchanged from Year 1. This is primarily due to the inherent risks remaining similar to Year 1 and the continued progress on new and existing mitigation measures in Year 2.

We will continue to build up from the residual risk mitigation roadmap committed to in Year 1, to address the residual risks. To target potential insufficiencies identified in the Year 2 Risk Assessment, we plan on improving our mitigation measures against P&C products in the following areas:

- **Enhancing effectiveness and accuracy of content moderation**: We will keep building up our moderation task force, hiring more human moderators to meet up with the volume of content moderation on non-compliant products on the Platform. We will also equip human moderators with better tools, developing automatic pop-up reminders for them to help refer to available information concerning the identified risk type, which will enhance the content moderation's effectiveness and accuracy.
- **Monitoring automatic penalties imposed on risky products:** We will implement a monitoring mechanism on the automatic penalties imposed on risky products detected by the Platform's risk control system. This monitoring mechanism will send early warnings on detected abnormal penalties or absence of penalty, which will ensure the timeliness and consistency of automatic penalties enacted by the system.
- **Enlarging the scope of applying image-identification algorithms in risk detection:** We will increase the usage of image-identification algorithms, particularly those specialised in detecting similarity between pictures, in our risk detection system, which will further enhance the risk detection effectiveness.
- **Building up the Platform's archive of product manufacturers and EU-responsible persons:** We will keep working on the implementation of the dedicated compliance project regarding the General Product Safety Regulation (EU/2023/988) (**GPSR**). We will enlarge the scope of information collection on product manufacturers and EU-responsible persons, and will communicate such information to consumers and regulators as required under the GPSR.
- **Upgrading recall notifications on dangerous products:** Based on the original recall notice process of informing concerned sellers and buyers, we will set up a new product recall notification channel to inform the authority's "Safety Business Gate" and also the product manufacturers regarding the Product safety issue.

VIII. Intellectual Property Rights

I. Risk Definition

In the IPR module, we have analysed the risk(s) that the Platform may be utilised to disseminate, or contribute to the dissemination of, "**IPR-infringing content**". AliExpress defines this as content that violates any rights related to Intellectual Property ("**IP**") rights, including copyright, trademarks, patents, design rights and geographical indications. Our IPR protection policies have been defined in accordance with applicable EU laws, including Directive 2001/29/EC ("**the Copyright Directive**"), Directive 2004/48/EC ("**the Enforcement Directive**") and Directive (EU) 2019/790 ("**the Directive on Copyright in the Digital Single Market**"). As outlined in the Year 1 Report, IPR covers:

- **Copyright infringements**, which are understood as any unauthorised use of copyrighted material such as text, images, videos, music, or software on the product or its packaging, as well as the unauthorised usage of copyrighted works on product listing(s).
- **Trademark infringements**, which includes the unauthorised use of a trademark on / or in connection with goods in a manner that is likely to cause confusion, deception, or mistake about the source of the goods. This covers the sale of counterfeit products.
- **Design infringements**, which includes the unauthorised use of a product appearance, shape or ornamentation protected by a design.
- **Patent infringements**, which covers innovations, including the unauthorised use of a product, service or process involving inventive step and industrial application protected by a patent.

In addition, considering the relevance of Alibaba's recent contribution to the 2024 Counterfeit and Piracy Watch List Public Consultation carried out by DG TRADE - Investment and Intellectual Property[10], [*replaced by footnote 10*], that expands on Alibaba IPR protection efforts and initiatives over the last two years, including regarding AliExpress.

II. Inherent Risk

Given the dynamic nature of the risk and the high volume of sellers attempting to list IPR infringing products, AliExpress has conducted a more in-depth analysis in Year 2, building upon the baseline of risk identified in Year 1. This analysis focuses on how various Platform features and factors, including those outlined in Article 34(2)(a) of the DSA, contribute to this risk.

a. Risks from Platform Design and Functionalities, including their misuse

As introduced in the Year 1 Report, the main source of IPR risks on online marketplaces is that users, specifically sellers, will attempt to disseminate IPR-infringing content by uploading or modifying

[10] https://circabc.europa.eu/ui/group/e9d50ad8-e41f-4379-839a-fdfe08f0aa96/library/bb3232d2-64cb-41f9-9e96-e0822a119956/details

product listings. [*Confidential*]. IPR-infringing content can be concealed among this information (e.g., using dashes between the letters of a trademarked brand).

There is a risk that sellers may post a seemingly innocuous listing to hide the sale of IPR-violating products. Other Platform functionalities may contribute to this risk. For example, buyers and sellers may misuse the IM functionality to provide details of the actual IPR-infringing product that is being sold. Further, users could share hyperlinks to violating goods, either on AliExpress' IM or on external platforms (so-called "hidden links"). In fact, due to AliExpress' success in combating counterfeits on the Platform, bad actors appear to have increasingly resorted to hidden link schemes that originate off-platform to leverage external platforms or other sites over which our safeguards do not apply.[11] Similarly, IPR-infringing products (as well as P&C Products) could be promoted through the Affiliate Program.

Another risk is that sellers may misuse the livestreaming function to draw attention to IPR-infringing goods. Beyond sellers, it's important to recognise that IPR risks can also be driven by buyers actively seeking to purchase infringing products. [*Confidential*]. Such strategies are often shared on external platforms, for example discussion forums on social media services.

In Year 2, our continuous monitoring of the EU risk environment identified two main events with potential impacts on IPR risks: the UEFA European Football Championship and the 2024 Paris Olympics[12]. These events were identified as posing a heightened risk of bad actors attempting to exploit the popularity of these sporting competitions to sell IPR-infringing products on the Platform, thereby violating the IPR of the rights holders.

b. Risks from Other Factors of the Platform (in line with Article 34(2) of the DSA)

Both in Year 1 and Year 2, we assessed how the factors listed in Article 34(2) of the DSA may influence IPR risks. Please refer to Section VI for more context on these factors.

- **Advertising systems and data practices:** There is an inherent risk that sellers will select IPR-infringing products to advertise. While it is not possible to assess the full scale of this risk, the historical volume of detected infringements can serve as a proxy for this particular risk. Among the 2,764,070 product listings removed by the Platform due to IPR violations in the time period from 1 July 2023 to 30 June 2024, 399,303 ([*Confidential*]) infringing product listings were advertised.
- **Content moderation systems:** AliExpress' content moderation systems are designed to reduce IPR risks. However, algorithmic detection systems may at times be unable to identify

[11] Please refer to **Annex 6**, i.e., Alibaba's recent contribution to the 2024 Counterfeit and Piracy Watch List Public Consultation carried out by DG TRADE - Investment and Intellectual Property, for more information regarding hidden links.

[12] The Global IP Enforcement Team had extensive engagement with Olympic representatives leading up to, and during, the Olympics to help ensure the maximum effect of proactive efforts and to expedite the removal of infringing product listings.

IPR-infringing content (e.g., in the case of insufficient training data). From 1 July 2023 to 30 June 2024, 687,127 product listings were removed for IPR violations through reactive means, in other words, they were not removed by the Platform's proactive moderation systems.

- **Recommender system:** There is a risk that some IPR-violating products, once published, may be recommended to users through our recommender system if sellers manage to evade our proactive content moderation tools. In the time period from 1 July 2023 to 30 June 2024, 1,272,175 products have been recommended and removed due to IPR infringements.
- **Relevant policies***:* As legislation gets updated in various countries, our IPR policy may become outdated and thus needs to be continuously iterated upon.

Given that we operate as a marketplace, the potential theoretical risk—assuming no controls are in place—of widespread dissemination of IPR-infringing products is "Medium High". While it is not possible to measure the risk without any controls in place, this risk can be estimated by examining the number of IPR holders whose rights may have been violated - from 1 July 2023 to 30 June 2024, 6,741 right-holders submitted 946,009 IPR notices to AliExpress. This risk can also be proxied by identifying the proportion of products involved in IPR infringements relative to the total number of listings on the Platform. From 1 July 2023 to 30 June 2024, 2,764,070 product listings were removed for IPR infringements [*Confidential*].

III. Existing Mitigations

In Year 2, we continued to operate strong control mechanisms and further enhanced our IPR controls through our Year 1 mitigation commitments. We also adapted them to address specific events that could act as IPR risk vectors in the EU.

a. Algorithmic Controls

The core of our IPR controls has not changed from Year 1. In terms of technological tools, we have algorithmic control systems in place to detect IPR-infringing products and AliExpress takes a proactive approach to detecting IPR violations. When a seller creates or modifies a listing, the listing contents are screened for suspicious content by our text-based, image-based, and combined indicators algorithmic systems. Flagged listings are reviewed by the IPR product review team and new infringements are included to the internal database of IPR-infringing elements that the algorithmic systems use to iteratively improve. Algorithmic quality assurance helps ensure that the algorithmic tools stay comprehensive and up to date with emerging risks and possible infringements. Algorithmic controls also check the similarities between new applicants and previous violators to prevent 'blacklisted' users from re-registering. In the period between 1 July 2023 to 30 June 2024, 75.1% of the total number of product listings removed for IPR violation were proactively removed by our algorithmic controls. Currently, we have over 2,000 brands in our brands database, which enables the training of our algorithmic systems to swiftly identify new product listings with potential IPR risks.

b. Internal Risk Identification

Our specialist teams are fundamental to ensure our policies are effectively enforced. Manual reviews are primarily managed by the CRO team, who may allocate specific tasks to specialised teams. For example, there are specialised teams that review algorithmic flags following a SOP that is regularly updated. AliExpress teams conduct weekly checks using product samples to proactively monitor and assess the prevalence of non-compliant products on the Platform. In addition, third-party teams perform independent sampling and analysis of products on the Platform and report their findings. As mentioned in Section VII (the P&C module), in addition to product-level checks, there are also account-level verifications. Sellers are required to undergo verification to review their qualifications as a trader and funding account information.

c. External Risk Identification

Beyond proactive detection, users (registered or unregistered; rights holders or not) have multiple avenues to report IPR infringements, including an email address (ipr@alibaba-inc.com), a notice form, and a dedicated IP protection portal for rights holders. Similar to our mitigation efforts for P&C Product risks, we further collaborate with external professional organisations (see Section VII on P&C module) to improve our enforcement of IPR policies.

d. Policies and Enforcement

Our relevant policies prohibit any posting or offering for sale of products that infringe on IP rights and set out appropriate penalties, should any infringement be identified. These policies are kept up to date with evolving risk vectors, as our teams actively monitor public opinion, regulatory changes, and other relevant factors. (For further information, please refer to Section VII - P&C Products.)

Additionally, our brand authorisation system has been developed to enhance our ability to inspect the documentation related to brand authorisation when a seller seeks approval to sell products from certain brands.

Case Study: Enhanced Guidelines for the Euro 2024 and the Paris Olympics
Recognising the potential for increased IPR violations during major international events, we have proactively engaged with rights holders, worked closely on exchange of know-how and information which enabled us to establish clear guidelines and controls to prevent the unauthorised usage or selling of protected content. We published two specific user guidelines (in Chinese) to address IPR issues related to these high-risk events this year, the Euro 2024 and the Paris 2024 Olympic Games. These guidelines, released in May 2024, indicated the wordmarks, image trademarks, host city logos, football jerseys, etc. that would constitute an infringement of IP rights linked to these events. The specific policies can be accessed through the following links:

- UEFA 2024 Guidelines
- Paris 2024 Olympic Games Guidelines

During the event enhanced-controls period, the following data was recorded:

- Number of listings reactively and proactively removed due to the Euro 2024 guidelines: 3,166
- Number of listings reactively and proactively removed due to the Olympics guidelines: 2,861

Among the removed listings, the number of listings removed reactively is 0 in both sports events, which suggests that our proactive detection mechanisms are functioning with strong efficacy.

User education and awareness can bolster safety on online platforms. AliExpress provides IPR training to users through programs like AliExpress Zhibei [13], which trains participating sellers to avoid unintended IPR violations. This training is provided through a continuous online program, with the publication dates for each section available on the AliExpress Zhibei website.

e. Advertising System and Recommender System Specific Controls

Regarding advertising systems, listings undergoing review by teams for potential violations are excluded from the advertising pool. For our recommender system, we implemented keyword blocking in the search function for a number of well-known and reputable brands at risk of having their products or brands infringed upon at their request. We also conducted internal assessments to prevent similar listings from appearing on the results page.

f. Content Moderation System Specific Controls

IPR risks related to content moderation systems are mitigated by regularly improving our IPR knowledge bases, which ensures that algorithmic systems are kept up to date. We also continuously refine the thresholds used in our detection algorithms. Furthermore, we monitor and aim to improve the proactive catch rate as a proxy for measuring algorithmic control effectiveness. IPR-related teams participate in rigorous training programs on IPR protection, including receiving training from right holders or from external legal consultants, typically arranged twice a year. There are internal trainings based on the updated IPR SOPs from time to time. Additionally, the appeals process gives users an avenue to contest moderation decisions if their content was inaccurately actioned for violating IPR.

g. New Mitigation Measures

In line with Year 1 commitments, we have, in the past twelve months, made significant improvements to the effectiveness of our mitigation measures. Notably:

[13] For access to AliExpress Zhibei, please click here.

- **Improved our Internal IPR-knowledge base**. We have enhanced our IPR knowledge base by providing rights holders with three dedicated portals to submit takedown notices. We are committed to further strengthening our collaboration with stakeholders to gather more data and improve our IPR enforcement capabilities. For instance, we added over 400 brands to our IPR-violations monitoring list between Year 1 and Year 2. Additionally, we receive regular feedback from rights holders through our participation in the EU Memorandum of Understanding on the Sale of Counterfeit Goods, effective from 2016. These enhancements to our IPR knowledge base ensure that our algorithmic control systems remain robust and effective.
- **Improved our IPR-violation detection algorithms**. We have continuously improved our IPR violation detection algorithms by incorporating the multimodal classification algorithm, which uses both text and images to identify risks more accurately by analysing and interpreting information from both textual and visual modalities. In September 2023, new algorithms for similar and identical product search were added, increasing the effectiveness of IPR protection. Additionally, we have integrated sellers' histories of suspicious behaviours and past IPR infringements into our algorithms, to enable more robust identification and prevention strategies against counterfeit products and abnormal pricing.
- **Stronger restrictions against abuse***:* Since December 2023, the IPR restriction rules differentiate between intentional and unintentional violations and we take stricter action against repeat infringements.
- **Choice service controls***:* Choice products undergo stricter controls than products sold by other sellers. Dedicated AliExpress teams curate and screen Choice sellers, to reduce the risk that IPR-infringing products will be published. In addition, under Choice's 'full-entrustment' model, most products will be placed within AliExpress-designated warehouses and manually inspected, with any violating products being withdrawn (read Section VII on P&C module for more details).
- **Voluntary recalls of infringing products***:* Since August 2023, we proactively recall products identified as IPR infringing to mitigate IPR risks. The Platform is also working to improve the timeliness of dispute resolutions for illegal products (including counterfeits) to under 2 business days.
- **Collaboration with professional service providers:** In 2024, in addition to considering buyer feedback and our analysis of referrer websites, we engaged in a partnership with a European service provider that specialises in IPR protection and detection of hidden links. This collaboration helps us identify and manage IPR risks by sharing intelligence to take enforcement actions, such as taking action against the related sellers on AliExpress as well as to report for removal, infringing content from third-party websites.

- **Strengthened controls against misuse:**
    - Since April 2024, to further mitigate the risk of IPR infringements arising from the Affiliate Program, once an infringement is discovered, AliExpress disconnects the product link shared by the affiliate, blocks any commissions for related orders, and suspends the accounts of repeat offenders.

- The CRO - Transaction Security team analyses the sources of traffic to the Platform once a month and checks if any are related to third-party websites that promote counterfeit products.

- **Updated policies**: As explained above, we produced guidelines for the UEFA Football Championship and the Paris 2024 Olympics to adapt to emerging risks related to IPR. These policies were enforced and during the duration of these events; 3,166 listings were removed under the UEFA Guidelines and 2,861 listings under the Olympic Guidelines, respectively.

IV. Residual Risk

Despite our best efforts to mitigate the risk of IPR-infringing products on the Platform through proactive and reactive measures, we cannot fully eliminate the risk due to the dynamic nature of the risk landscape, where new illegal products may arise and malicious sellers and buyers may be motivated to transact IPR-infringing products. Furthermore, hidden link schemes originate outside of our Platform where our safeguards cannot be applied. Our efforts to mitigate risk are made more complex by the volume of newly added listings, our global user base and the continuously and rapidly evolving strategies to distribute IPR infringing and counterfeit goods. Consequently, a certain level of residual risk persists on the Platform.

Based on the inherent risk score and mitigation effectiveness score of this risk module, the residual risk score is qualified as “Low Medium”. Nonetheless, we continue to work towards minimising the risk of disseminating IPR-infringing products through the Platform.

Inherent Risk	**Mitigation Effectiveness Score**	**Residual Risks**
Based on the probability and severity scores calculated using the DSA Risk Assessment Rating Methodology, the inherent risk score is assessed as “**Medium High**”, which indicates that there is a relatively high probability of the risks occurring during the provision of the service, and they have obvious negative impacts on users.	Overall, the mitigation implementations are effective and resulted in a decreased exposure of non-compliant content on the Platform. The mitigation effectiveness score is calculated to be “**Strong**” (71%), which indicates minimal likelihood of a control failure.	Based on the inherent risk score and mitigation effectiveness score, the residual risk remains “**Low Medium**” on the Platform, which indicates a moderately low level of concern around the likelihood or impact of risks arising to users on the Platform after mitigation measures have been applied.

V. Conclusion and Future Mitigations

In Year 2, the residual risk rating of “Low Medium” has remained unchanged from Year 1. This is primarily due to the inherent risks remaining similar to Year 1 and the continued progress on new and existing mitigation measures in Year 2.

To address the residual risks, we will continue to build up from the residual risk mitigation roadmap committed to in Year 1. Targeting potential insufficiencies identified in the Year 2 Risk Assessment, we plan on improving our mitigation measures against IPR risks in the following areas:

- **Increased penalties for policy violations:** For more severe IPR infringement violations, we will increase the financial penalties deducted from the seller's performance security deposit to improve the effectiveness of our policy enforcement.
- **Strengthened cooperation with brand rights holders:** We will launch the Brandsafe project to provide tools and data insights about counterfeit goods control for brand rights holders in order to collaboratively tackle the spread of counterfeit goods.

IX. Content Compliance

I. Risk Definition

In the Content Compliance ("**CC**") module, AliExpress analysed the risk(s) that the Platform may be used to disseminate, or contribute to the dissemination of, harmful and illegal user-generated content ("**UGC**") beyond the scope of the P&C and the IPR modules. The CC module analyses the risks that UGC in whatever shape or surface – i.e. text or images in product reviews, IM messages, etc. – may contribute to the dissemination of illegal content as well as negatively impacting fundamental rights that may manifest through the sharing of UGC, including non-discrimination, and protection against gender-based violence. Content Compliance module includes an analysis of the dissemination of UGC that follows EU and other European laws and regulations, including the 2008/913/JHA Framework Decision ("Framework Decision on combating certain forms and expressions of racism and xenophobia by means of criminal law"), Regulation (EU) 2021/784 ("Regulation on Terrorist Content Online") Directive (EU) 2011/93 ("Directive on Combating the sexual abuse and sexual exploitation of children and child pornography"), Directive (EU) 2024/1385 ("Directive on combating violence against women and domestic violence") and the Council of Europe Convention on preventing and combating violence against women and domestic violence. UGC that violates AliExpress' Terms and Conditions as well as policies is hereafter referred to as "non-compliant content".

As outlined in the Year 1 Report and the Community Guidelines, non-compliant content covers:

- **Illegal hate speech and unlawful discriminatory content:** Any kind of communication in speech, writing or behaviour, that attacks or uses pejorative or discriminatory language with reference to a user (buyer or seller) or a group on the basis of who they are e.g., based on religion, ethnicity, nationality, race, colour, descent, gender or other identity.
- **Harms to human dignity:** Any kind of content that is libellous, defamatory, harassing, threatening, insulting, obscene, pornographic, obscene, offensive, untrue, false, exaggerated or misleading.
- **Terrorist content:** Any kind of content that promotes, celebrates, or justifies terrorist activities, ideologies, or propaganda. This includes content that advocates violence, glorifies terrorist acts or individuals, or spreads hate speech and slogans associated with terrorism.
- **Public security:** Any kind of content that endangers national sovereignty and security, advocates for wars or military conflicts, disseminates violence, or promotes the misuse of illicit drugs or chemicals.
- **Child sexual abuse material** ("**CSAM**"): Any kind of sexually explicit images or descriptions or pornographic and vulgar content around children.
- **Harm to cultural, religious and linguistic diversity:** Any kind of content that incites ethnic hatred and discrimination.
- **Gender-based violence and Non-consensual sharing of private images:** Any kind of content that advocates for violence against women, doxxed individuals, or fabricates false information to damage the reputation of others.

II. Inherent Risk

Between Year 1 and Year 2, the Content Compliance risk landscape has remained stable. In Year 2, we conducted a more in-depth analysis of how different Platform features and factors (including those listed in Article 34(2)(a) of the DSA may contribute to the risk.

a. Risks from Platform Design and Functionalities, including their misuse

Content issues on AliExpress primarily stem from information related to non-compliant products that are identified during the product control process, which will be deleted. Beyond that, UGC creates additional content-related risks on the Platform. We offer a variety of interactive features designed to enhance the user experience but these also may pose risks. Features such as customer reviews, Q&A sections, and IM can be misused to disseminate non-compliant content, including hate speech, explicit images, and illegal product information. Customisation options for user profiles and stores, along with marketing tools like push notifications and email marketing, also carry the risk of promoting non-compliant content. Additionally, the Affiliate Program and livestreaming features present specific issues in controlling the spread of non-compliant content, particularly given the potential for off-platform transactions and the real-time nature of live broadcasts.

There is a risk that users may misuse the Platform functionalities to publish non-compliant content and avoid detection. This may occur through attempts to evade keyword and image detection by manipulating images and text. Additionally, abuse of the Platform's IM or chat features could involve the use of bots to generate spam or harass users.

b. Risks from Other Factors of the Platform (in line with Article 34(2) of the DSA)

Both in Year 1 and Year 2, we assessed how the factors listed in Article 34(2) of the DSA may influence the risks of disseminating harmful content. Please refer to Section VI for more context on these factors.

- **Advertising systems and data practices***:* There is an inherent risk that sellers could use AliExpress' advertising systems to publish non-compliant advertising content (e.g., in the product photo, product description, etc). From 27 May 2024 to 26 August 2024, we blocked or deleted 1,062,965 advertisements due to non-compliant content, [*Confidential*].[14]
- **Recommender system:** There is a risk that AliExpress' recommender system, by means of search keywords and ad words, could potentially expose or disseminate prohibited content, as it may inadvertently amplify and recommend non-compliant or harmful content if certain keywords gain traction among users. From 6 August to 25 August 2024 we have blocked or deleted 8,337,262 non-compliant content recommended by AliExpress' recommender systems [*Confidential*].[15]

[14] Our system log stores data for only the past three months in this respect.

[15] The relatively shorter data period is due to the storage time limit of our system logs in the EU.

- **Relevant policies***:* As legislation gets updated in various countries, our Content Compliance policy could become outdated and thus would need to be continuously iterated upon. At the policy enforcement level, the effectiveness of implementing Platform policies is influenced by various factors such as risk control tools, technical capabilities, and human resources, which may experience errors and failures. Between 1 July 2023 and 30 June 2024, we have updated our AliExpress Community Guidelines once for these purposes.
- **Content moderation systems:** Our content moderation systems are designed to reduce risks around non-compliant content. However, algorithmic detection systems could fail to identify infringing content (e.g., in the case of insufficient training, particularly on diverse languages). The number and expertise of manual reviewers could also be insufficient to promptly and accurately handle flagged content. Additionally, there may be challenges in moderating real-time situations like IM or livestreaming. In this regard, the number of non-compliant content detected through reactive reports from 1 July 2023 to 30 June 2024 is 11,682.

Given that AliExpress operates as a marketplace, the spread of violating content (different from product listings) is a comparatively less prevalent risk. Assuming no controls were in place, the potential theoretical risk of widespread dissemination of non-compliant content is “Very Unlikely”. While it is not possible to measure the risk without any controls in place, this risk can be estimated by considering the total amount of content proactively blocked and reactively removed worldwide. For example, from 27 May 2024 to 26 August 2024, the total number of non-compliant user-generated content blocked or removed amounted to 6,234,972 [*Confidential*].

III. Existing Mitigations

In Year 2, we continued to operate strong control mechanisms and further enhanced our content controls through our Year 1 mitigation commitments. The mitigation measures can be grouped into several key areas: the overall process for content compliance risk identification and mitigation, the tools developed for specific mitigation purposes, and the taskforce and their management.

a. Detection Mechanisms: Automated Blocking and Manual Review

We have two risk control mechanisms, pre-live and post-live, to ensure that prohibited content is identified and blocked automatically and in a timely manner.

Pre-live system

The pre-live system acts as the first line of defence, where content is automatically reviewed against a combination of restricted keywords, algorithms, and risk behaviour indicators to effectively identify non-compliant content before it is published. These algorithms are designed to identify and block content that violates Platform policies. For instance, by extracting text from images and cross-referencing it with a database of restricted keywords, or by assessing visual content for elements associated with known violative content. Risk management personnel will also conduct manual checks on the generated results.

Post-live system

For most professional and user-generated content, our risk management system operates as a pre-live mechanism, requiring all content to pass through the system before being published online. [*Confidential*]. In these channels, where an instant response is required, content is published online first and then taken down if it is identified as non-compliant content. This approach balances the user preference for swift content publication with the need to mitigate non-compliant content dissemination.

b. Policies and Enforcement

Policy enforcement is a critical aspect of our content compliance strategy. The Platform has developed a comprehensive set of policies, outlined in our Community Guidelines and specific policies for different channels like AliExpress Live. In professional and user generated content channels, users must follow these policies. These policies are designed to cover a wide range of content-related risks, from hate speech and terrorist content to public security threats and non-consensual activities, and are monitored to ensure coverage of potential crisis scenarios, new risk trends and to align them with relevant EU and member states' legal requirements. Enforcement measures include immediate content blocking, temporary restriction on posting of content, manual reviews of high-traffic content, and more severe penalties for users who repeatedly violate the rules. For severe violations, AliExpress may disable user accounts temporarily or permanently, depending on the nature and frequency of the infractions. For livestreams, the Platform also stipulates onboarding requirements in order that only reputable sellers and influencers are allowed to use this channel.

c. Enhancements to Proactive Controls

We monitor the algorithms' predicted violation scores and other performance indicators of the detection algorithm, which are used to enhance our proactive mitigation strategies.

The monitoring of the performance of the proactive controls allows us to enhance the effectiveness of the automated risk detection and blocking mechanisms by continually optimising the risk management systems, strategies and algorithms. For instance, risk management personnel provide restricted keywords and detected prohibited content as a training dataset to the algorithm team to improve text algorithm performance. To enhance detection performance, risk behaviour indicators are used alongside algorithms, such as by correlating specific non-compliant keywords with searches for related product categories to expand recall rate.

d. Strong Reactive Controls

The manual review team is tasked with manually reviewing content that has been flagged by the system but not conclusively identified by automated systems as non-compliant. By combining automated detection and manual verification, we aim to effectively mitigate the risk of non-compliant content being disseminated across all professional and user generated content channels on AliExpress. Additionally, we have reporting channels available on the Platform, and relevant teams (including the customer service team, the internal inspection team, and the public sentiment team) are involved in

the monitoring and discovery of residual non-compliant content. The risk management team collects and verifies reports and cases, then takes down the non-compliant content accordingly. From 1 July 2023 to 30 June 2024, the number of non-compliant content items detected through reactive reports amounted to 11,682. During the same period, there were 55 successful appeals worldwide for compliant content that were wrongly enforced.

e. Measures Against Risk of Reappearance of Non-Compliant Content

We also take proactive steps to prevent the reappearance of non-compliant content. The Platform channels new violation data into a structured online library, which helps in identifying emerging risks and keeping an updated database of prohibited keywords. Stricter penalties are imposed on repeat offenders, and mechanisms are in place to prevent banned sellers from re-registering on the Platform.

f. New Mitigation Measures

In line with Year 1 commitments, we have, in the past twelve months, made significant improvements to the effectiveness of our mitigation measures. Notably:

- **Enhanced our risks controls and SOPs**: We have conducted a thorough assessment of our content risk controls, updated the content risk register and scope, and enhanced the internal SOPs for managing content risks. Between 1 July 2023 and 30 June 2024, we have updated these content risk control SOPs 26 times, covering risk areas such as public security, CSAM and pornographic content, etc. The updates involved clarifying grey area cases to ensure more accurate policy enforcement while safeguarding user experience.
- **Increased our complaint and appeal mechanisms for non-registered users**: We have also provided easily accessible appeal and complaint portals for users to make reports and challenge moderation decisions. In particular, this year we launched a notice submission tool aimed at non-registered users (but also open to registered users), available on the Platform (accessible from the site footer) to facilitate the submission of notices about any non-compliant content on the Platform by non-registered users. When the reporting party submits a report through the general online notice submission form, the system immediately sends an automated email to confirm receipt of the report. The report is reviewed by the relevant competent team. Once a decision is made, we communicate this to the reporting party by email. The reporting party can also query the status of the notice using the report ID, through the following link on our website (for non-registered users). In case of successful appeals, we have updated processes to quickly restore content.
- **Updated our algorithmic detection capabilities:** We launched a new text algorithm model for detecting illegal content, optimised for pornographic and vulgar content, information on illegal provision of services. [*Confidential*] In July 2024, through a combination of algorithmic detection and subsequent manual review, we found and deleted 62,206 illegal pieces of content through this algorithm. We are also developing a multilingual text algorithm incorporating EU languages based on a Natural language processing model (NLP). This NLP has

expanded the language list of our risk management system and will allow for more localised control of risks in more countries (e.g., detecting risks from slang).

- **Additional human content moderators:** To enhance our human moderation capabilities, we have added 6 human moderators focusing on non-English content (specifically, Spanish, Portuguese, French and German). Also, the content moderation team for recommended keywords has increased [*Confidential*].
- **Introduced moderation for AI Generated content**: The rapid growth of AI-generated content (AIGC) in text and image formats may pose significant challenges to our risk management system. To address this, we have deployed algorithms designed to detect and mitigate content compliance risks by monitoring inputs (user-provided context) and outputs (AI-generated text and images). If compliance risks are detected, AI-generated results are blocked to ensure content safety.

IV. Residual Risk

Despite our best efforts to mitigate the risk of the dissemination of harmful and illegal user-generated content on the Platform through proactive and reactive measures, we cannot fully eliminate the risk due to the dynamic nature of the risk landscape, with motivated malicious actors spreading such content and the continuously evolving nature of the strategies used to evade our controls. Our efforts to mitigate this risk are further complicated by the multiple avenues of content dissemination, the diverse global user base, and the avenues for instant sharing of content on the Platform. Consequently, it is evident that a certain level of residual risks persists on the Platform. Based on the inherent risk score and mitigation effectiveness score of this risk module, the residual risk score is qualified as "Low". Nonetheless, we continue to work towards minimising the risk of disseminating such content through the Platform.

Inherent Risk	**Mitigation Effectiveness Score**	**Residual Risks**
Based on the probability and severity scores calculated using the DSA Risk Assessment Rating Methodology, the inherent risk score is assessed as "**Low Medium**", which indicates that the probability of the occurrence of risks is low, and they have the potential to have a low impact on users.	Overall, the mitigation implementations are effective and resulted in a decreased exposure of non- compliant content on the Platform. The mitigation effectiveness score is calculated to be "**Moderate**" (60%), indicating minor likelihood of a control failure.	Based on the inherent risk score and mitigation effectiveness score, the residual risk remains "**Low**" on the Platform, which indicates a low level of concern around the likelihood or impact of risks arising to users on the Platform after mitigation measures have been applied.

V. Conclusion and Future Mitigations

In Year 2, the residual risks rating of "Low" has remained unchanged from Year 1. This is primarily due to the inherent risks remaining similar to Year 1 and the continued progress on new and existing mitigation measures in Year 2.

We will continue to build up from the residual risk mitigation roadmap committed to in Year 1, to address the residual risks. We plan on improving our mitigation measures against Content Compliance risks in the following areas, to target potential insufficiencies identified in the Year 2 Risk Assessment:

- **Strengthening our detection capabilities:** We plan to continue strengthening our detection capabilities for emerging risks by expanding reporting channels for more risk scenarios. We will also continue to optimise our content risk algorithms to improve our risk control capabilities. Specifically, we will develop a large redline text model to improve prevention and control capabilities under scenarios of multi-languages and small amounts of samples and to improve risk recall levels. To improve the overall accuracy of algorithmic controls, we will adopt the approach of leveraging both keyword identification using traditional models and large language models. We will also analyse similar semantic and search behaviours to proactively discover new non-compliant content with similar risks to known non-compliant content.
- **Enhance controls around fake ratings, fake reviews and spam messages:** We will strengthen controls against non-compliant content arising from fake ratings, fake reviews and spam messages specifically. On fake ratings and reviews, we will continuously collect data and analyse the behaviour patterns of click farming, and optimise the algorithm recognition logic and accuracy of fake user reviews identification. Meanwhile, we will revise the penalty rules and strengthen the removal of merchants who have been identified as engaging in click farming. On spam messages, we will focus on enhancing our capabilities to identify and block spam advertisements by improving our text and image similarity algorithms, and algorithmic detection of abnormal mailboxes and gangs.
- **Enhance our tiered penalty system:** We plan to implement a more targeted governance approach for repeated violations across a broader range of content scenarios. By adopting a layered penalty system, we aim to effectively reduce the risk of repeated violations. This may involve measures such as blocking/deleting content, disabling the ability to publish content, suspending accounts, and permanently closing accounts for repeat offenders.

X. Data Protection

I. Risk Definition

In the Data Protection module, we have analysed the risk(s) relating to the processing, storage and usage of personal data on the Platform. Our definition of '**personal data**' is drawn from the GDPR (as defined below) and refers to any information relating to an identified or identifiable natural person (**'data subject**'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Our data protection policies were defined in accordance with applicable EU laws, including the **EU General Data Protection Regulation** (GDPR), **EU Charter of Fundamental Rights**, **European Convention on Human Rights**, and the **European Court of Human Rights Decisions**. As defined in the Year 1 Report, Data Protection covers:

- **Protection of personal data**, which is understood as the protections around the collection, use, disclosure, storage, and deletion of personal information by the Platform.
- **Right for Respect for private and family life**, which, in accordance with the ECHR cases, is understood as respecting a person's name, gender, sexual orientation and sexual life, and also information about a person's health, ethnic identity and racial origin, right to their image, and their biometric information, including DNA samples, profiles, or fingerprints.

II. Inherent Risk

Between Year 1 and Year 2, the Data Protection risk landscape has remained stable. In Year 2, we deepened the analysis of how different Platform features and factors (including those listed in Article 34(2)(a) of the DSA) may contribute to the risk.

a. Risks from Platform Design and Functionalities, including their misuse

In the context of data protection, the various functionalities of the Platform present potential for risks if not carefully managed. As a global marketplace, AliExpress facilitates transactions between buyers and sellers, which necessitates the exchange of personal information. While this exchange is essential for the Platform's operations, it also introduces the risk of misuse or unauthorised access to user data.

We also operate in multiple regions with varying data protection requirements, meaning that the transfer of personal data across borders is an important area of focus. Data transferred to third-party countries (namely countries outside of the European Economic Area) without proper controls in place may pose risks such as cyber-attacks and data breaches.

In addition, partnerships with third parties on the Platform who offer users products and services not offered directly by AliExpress (including payment service providers such as Alipay) or other companies in the Alibaba Group present another layer of complexity. While these collaborations are essential for fulfilling a transaction or for offering a broad range of services, they may be subject to Privacy Policies

different from AliExpress' own. The risk may arise for users responding to a service offered by these third parties on AliExpress without realising the different treatment of their personal data by these parties.

There is also a risk that users may misuse the Platform functionalities to create risks to other users' data. The seller operations platform provides data to sellers in order to help them fulfil orders, however it may potentially be misused by sellers who could leak said data. Additionally, external crawlers, cyberattacks on user accounts, and malicious hyperlinking by users could expose personal data to unauthorised access, leading to concerns for users if no controls were in place.

b. Risks from Other Factors of the Platform (in line with Article 34(2) of the DSA)

Both in Year 1 and Year 2, we assessed how the factors listed in Article 34(2) of the DSA may influence Data Protection risks. Please refer to Section VI for more context on these factors.

- **Advertising systems:** The processing of user data for targeted advertisements on AliExpress, including the analysis of users' buying and browsing behaviour, may pose privacy risks if not properly controlled in a transparent manner. Without adequate controls, the basis for this data processing could be undermined.
- **Recommender system:** While designed to personalise user experiences by tapping into shopping habits, recommender systems carry the risk of exposing users to undesired recommendations, creating the perception of privacy intrusions. This being said, users can turn off personalisation themselves, but can also ask the Platform to do it for them. Between 1 July 2023 to 30 June 2024, only 3 EU users exercised Data Subject Right Requests ("**DSRs**") asking Platform to turn off the personalised recommendation function.
- **Policies:** As legislation gets updated in various countries, our Data Protection policy may become outdated and may need to be continuously iterated upon to ensure it is up to date.
- **Data Protection and content moderation systems:** While data protection systems on AliExpress are essential for mitigating risks, they themselves can introduce vulnerabilities if not properly implemented or managed, with potential risks arising around the storage, anonymisation, management, encryption, and security of data if no controls were in place.

Assuming no controls were in place, the potential theoretical risk of widespread data protection related infringements is "Medium-High". While it is not possible to measure the risk without any controls in place, this risk can be estimated by considering the proactive data protection safeguard as proxied by the number of users who exercised their data rights. For example, during the period from 1 July 2023 to 30 June 2024, [*Confidential*] users closed their accounts, representing 0.56% of registered EU accounts.

III. Existing Mitigations

In Year 2, we continued operating strong control mechanisms and further enhanced our Data protection controls through our Year 1 mitigation commitments. The mitigation measures can be grouped into several key areas: the tools developed for proactive risk mitigation, the task force and

its management, internal and external risk identification methods, and the relevant risk mitigation workflows.

a. Technical Controls

We have implemented several mechanisms to enhance data protection and mitigate privacy risks. We have introduced an anonymisation and encryption system [*Confidential*]. This system allows sellers to use a specific [*Confidential*] for package sending instead of direct access to consumers' delivery information in plain form, thereby reducing the risk of privacy breaches. To further protect users' data, we allow sellers' access to buyers' personal information for only 90 days, and, for semi-fulfilled and participating-warehouse-shipped orders, sellers are not able to view the buyer's personal information.

Additionally, we utilise data partitioning tools to further mitigate risks, and we classify data assets by assigning security scores based on confidentiality, integrity, and availability, categorising them into four security levels. This classification allows us to prioritise protective measures according to the sensitivity and importance of the data. Our content moderation systems play a crucial role in mitigating data protection risks by actively monitoring and filtering content. For instance, our traffic risk identification system is designed to detect and manage bot traffic, including the malicious scraping of sensitive personal information.

To protect against external data scraping and malicious cyber-attacks, we ensure that personal data is anonymised when possible. For instances where non-encrypted transmission is required, we assess the need for Distributed Denial of Service (DDoS) protection and anti-crawling measures. Additionally, we leverage Alibaba's traffic cleaning software, anti-intrusion firewalls, and an early warning system to monitor and respond to potential threats in real time. Our anti-crawler systems and Web Application Firewall are specifically deployed to block unauthorised bot access to interfaces containing personal data. This aims to ensure that only legitimate requests are processed.

b. Policies and Enforcement

Our Privacy Policy is a key component in mitigating data protection risks on AliExpress. It clearly outlines how we collect, process, store, and transmit personal data in compliance with GDPR principles of lawfulness, fairness, and transparency. By detailing the types of information we collect and the contexts in which it is processed, we empower users to understand and control their data. The policy covers essential areas such as information collection, data retention, user rights, security measures, and international data transfers, making sure users are informed and can exercise their rights, including requesting data deletion or opting out of personalised ads.

AliExpress makes its Privacy Policy easily accessible through multiple channels, including the portal and app settings, so users can fully understand how their data is handled. AliExpress users can exercise their data subject rights via the Privacy Centre or by contacting the Data Protection Officer (DPO). For instance, users can delete their accounts, unsubscribe from marketing messages, or turn off personalised ads. Additionally, we display to EU users a cookie banner, allowing them to refuse data

collection by cookies and other similar technologies. Between 1 July 2023 to 30 June 2024, we received 496,852 EU user Data Subject Right Requests (DSRs) requesting the Platform to delete personal accounts, unsubscribe from marketing messages, etc., which received a 100% response rate.

When users register with AliExpress, we will disclose what information is collected and its purpose, as stated in our privacy policy. If the privacy policy is adjusted, users can access the latest and the previous version of the Privacy Policy at any time. In some cases when we make major revisions to the key terms of the Privacy Policy, users will be informed of these changes and will be prompted to read and agree to the new terms.

c. Verification Processes

To prevent the misuse of anonymous or fake accounts, we implemented strong buyer and seller verification processes. Buyers are required to create secure passwords and verify their identity via phone or email. Sellers, especially those targeting EU consumers, undergo a robust onboarding process where we collect and verify key information, including business details and their undertaking to only offer products that comply with the applicable EU laws. Since March 2024, we have further strengthened these controls by directly collecting additional information about the registration authority for sellers during the onboarding process.

We also enforce strict security measures for third parties that may access user data. This includes conducting data due diligence and making sure all collaborating third parties sign a Data Processing Agreement where applicable. We adhere to the principle of sharing only the minimum necessary user data with third parties to maintain security and privacy throughout our collaborations.

d. Internal Controls

We have designated a dedicated “Data Security Compliance Team” responsible for overseeing personal information protection. This team formulates and maintains policies related to data security, including the protection of personal information. Additionally, we have a “Compliance Risk Management Team” to ensure the legality and compliance of all data security-related matters.

e. External Audits

We engage with external agencies, including the British Standards Institution (“BSI”), to conduct annual audits of our information security and privacy management practices. These audits cover our products, development, testing, and operational processes. During this past year we maintained our ISO 27001 and ISO 27701 certifications, as confirmed by the BSI, reflecting our ongoing commitment to maintaining high standards in data privacy and security.

f. Additional Controls

Data Transfers

We take significant steps to mitigate data protection risks associated with the transfer of EU users' personal data to non-EU countries. To ensure legal compliance, these data transfers are conducted based on the necessity of fulfilling contracts between users and the Platform, the use of Standard Contractual Clauses (SCCs) approved by the European Commission, and/or explicit user consent. We have also made efforts to minimise international data transfers by promoting the use of EU-based warehouses, which not only enhances the user experience and speeds up logistics but also reduces the number of logistics providers involved, thereby lowering the risk of data breaches. The personal data of EU users is securely stored within the EU, specifically in a data centre located in Germany, with cross-region crisis recovery back-ups in Singapore and the United States.

To protect the data of EU users under the Choice service, we have taken specific steps to limit sellers' access to buyers' personal information under the Choice service. For orders under the Choice service where the cooperating warehouse handles logistics, sellers only see the warehouse address rather than the buyer's personal details, keeping that information more secure.

Privacy Risks from Third Parties

To mitigate privacy risks associated with third-party partners, we clearly inform users in our Privacy Policy that we have relationships with other parties and websites to offer products and services that we do not directly provide. We explicitly state that the AliExpress Privacy Policy does not apply to these third-party or co-branded sites, and we advise users to review the relevant privacy policies of these sites before engaging with any offers, products, or services they advertise.

g. New Mitigation Measures

In line with Year 1 commitments, we have, in the past twelve months, made significant improvements to the effectiveness of our mitigation measures. Notably:

- **Enhanced user control of personalised recommendation systems:** We have enhanced our personalised recommendation system, giving users greater control over their experience. Users can now turn off personalised recommendations in our Privacy Centre and select specific types of push notifications they wish to receive, such as order updates, promotions, activities, and interaction alerts. Additionally, through the Cookie Preferences, users can customise their data collection preferences, including choosing whether to accept specific types of cookies to collect their own data, such as users can choose to reject advertising cookies.
- **Limiting seller's access to buyer's personal information in order page**: In March 2024, we updated the Seller's Centre and completed the order-level anonymisation of buyer details in the orders page viewable by sellers. For instance, sellers cannot view personal information in orders that were completed over 90 days ago and in orders that the participating warehouse is responsible for sending the products to the relevant buyers, helping to reduce unnecessary data exposure. This update minimises unnecessary disclosure of buyer information, further mitigating data protection risks.
- **Development of personal data identification and protection system:** We are actively developing a personal data identification and protection system to continuously enhance data

privacy through the identification, classification, control, and auditing of data assets, alongside raising awareness and education on these topics. AliExpress has established a data security platform that categorises and labels personal data, and we are currently optimising the Platform to further improve personal data usage and protection.

- **Third-party education and data protection policy:** We provide education and training on "personal information protection" for third parties, including logistics and customer service providers, who may access or handle our users' personal information. The training covered key definitions, such as personal data, and provided guidance on data storage, transmission, and processing. Additionally, we have established the "AliExpress Supplier Data Protection Requirements" policy. We plan to continue offering regular training sessions, either bi-annually or annually, to reinforce these practices and ensure ongoing compliance with data protection standards.
- **Optimisation of data subject right request handling**: AliExpress has further optimised the relevant SOP to better protect the rights of data subjects and enhance the response time and processing effectiveness for related events. The updated SOP now includes detailed processing steps, transfer processes, and designated responsibilities for each type of data subject right request. For instance, when a user requests to disable personalised recommendations, the receiving staff will create an internal processing work order, which is then assigned to the appropriate team. Once the technical processing is completed, a designated representative will promptly notify the user that their request has been fulfilled.

IV. Residual Risk

Despite our best efforts in mitigating the risks related to Data Protection on the Platform through proactive and reactive measures, we cannot fully eliminate the risk due to the possibility of misuse or unauthorised access to user data by sellers (who may require access to user data to fulfil orders). Our efforts to mitigate this risk are further complicated by further risks due to potential vulnerabilities that may arise throughout the data lifecycle. Consequently, it is evident that a certain level of residual risks persists on the Platform. Based on the inherent risk score and mitigation effectiveness score of this risk module, the residual risk score is qualified as "Low-Medium". Nonetheless, we continue to work towards minimising the risk of unauthorised access, transmission and use of data.

Inherent Risk	**Mitigation Effectiveness Score**	**Residual Risks**
Based on the probability and severity scores calculated using the DSA Risk Assessment Rating Methodology, the inherent risk score is assessed as "**Medium High**", which Indicates a relatively high concern around the probability of risks occurring that may have the potential to cause negative	Overall, the mitigation implementations are effective and resulted in a decreased exposure of such risks on the Platform. The mitigation effectiveness score is calculated to be "**Strong**" (73%), which indicates	Based on the inherent risk score and mitigation effectiveness score, the residual risk remains "**Low-Medium**" on the Platform, which indicates a moderately low level of concern around the likelihood or impact of risks arising to users on the Platform

impacts to the users	minimal likelihood of a control failure.	after mitigation measures have been applied.

V. Conclusion and Future Mitigations

In Year 2, the residual risk rating of "Low-Medium" is reduced from the rating of "Medium" in Year 1. Notably, we have updated the Year 2 methodology for calculating the risk probability to be more accurate and relevant by considering the number of EU users exercising their data rights, instead of considering the number of days where ESU events took place over a year. The reduced rating could also be due to the continued progress on new and existing mitigation measures in Year 2.

We will continue to build up from the residual risk mitigation roadmap committed to in Year 1, to address the residual risks. We plan on improving our mitigation measures against Data Protection risks in the following areas, to target potential insufficiencies identified in the Year 2 Risk Assessment:

- **Ensuring enhanced monitoring of our data systems**: We will continue to invite external monitoring agencies to audit information security and privacy security management, such as BSI to inspect our products, development, testing and operation processes every year.
- **Enhancing oversight of third parties on the Platform:** We will build a Third Party Risk Management mechanism to further enhance our oversight of Third Party data security protection capabilities.

XI. Consumer Protection and Related Fundamental Rights

I. Risk Definition

In the Consumer Protection and Related Fundamental Rights module, we analysed the risk(s) that the Platform functionalities may be utilised to undermine consumer rights and other related fundamental rights of the recipients of AliExpress's services. We have defined our scope of consumer rights protection and other related fundamental rights protection in accordance with applicable EU laws, including **the EU Charter** (2000/C364/01), with particular reference to Article 38 of the Charter. As previously outlined in the Year 1 Report, risks incorporated in this module are particularly diverse in nature, and are related to various types of services provided by AliExpress. In the Year 2 Report, we have identified the following risk areas:

- **Sale of products or provisions of services in infringement of consumer protection law,** which is understood as situations where a business or individual sells goods or offers services in a manner that violates laws designed to protect consumers. These infringements include false advertising, selling defective products, providing unfair contract terms, applying deceptive pricing, failure to provide necessary information, and other unfair business practices that exploit, deceive, or disadvantage consumers.
- **Online stalking,** which is understood as the use of digital communication tools (such as instant messaging or commenting on product reviews) to harass, intimidate, or surveil an individual repeatedly. This behaviour can include sending threatening messages, spreading false information, or monitoring someone's online activities without their consent.
- **Rights of the Child & Protection of Minors,** whereby the Rights of the Child include the right to life, education, healthcare, protection from abuse and exploitation, and the right to express their views. The protection of minors involves safeguarding children from physical, emotional, and psychological harm, making sure their fundamental rights are upheld in all aspects of life, including education, family, and online environments.
- **Online interface design that may stimulate behavioural addictions of recipients of the service,** which is understood as the design that intentionally or unintentionally encourages addictive behaviours in users.
- **Right to effective remedy and to fair trial,** which is understood as the fundamental right that ensures individuals can seek justice when their rights have been violated. An effective remedy includes access to a competent legal authority that can provide redress, such as compensation, restitution, or other forms of justice. The right to a fair trial guarantees that legal proceedings are conducted impartially, without undue delay, and with respect for the legal rights of all parties involved, including the right to be heard and to present evidence.
- **Risk to public health,** which is understood as any situation, behaviour, or substance that poses a threat to the physical and psychological health and well-being of the general population, which includes the spread of infectious diseases, exposure to harmful environmental factors, unsafe products, or practices that compromise the safety of food, water, air, or other essential resources.

- **Freedom of expression and information,** which is understood as the fundamental right that allows individuals to freely express their thoughts, opinions, and ideas without fear of censorship or retaliation.
- **Freedom to conduct a business,** which is understood as the fundamental economic right that allows individuals and companies to pursue economic activities, establish and run businesses, and enter into contracts without undue interference from the state or other entities. This right includes the ability to produce, trade, and offer services in a competitive market, subject to the laws and regulations that ensure fair competition, consumer protection, and public interest.

II. Inherent Risk

Between Year 1 and Year 2, the Consumer Protection risk landscape has remained stable. Nonetheless, in line with the strengthened methodology, we conducted a more in-depth analysis of how different Platform features and factors (including those listed in Article 34(2)(a) of the DSA) may contribute to the risk, with special attention to new features or updated features deployed on the Platform after the Year 1 Risk Assessment.

a. Risks from Platform Design and Functionalities, including their misuse

Consistent with the analysis in the Year 1 Report, the main source of risks for consumer rights and protection and other fundamental rights is that users, specifically sellers, may attempt to bypass Platform rules or exploit Platform design and functionalities to unfairly benefit themselves. In the process, they may impose financial losses or cause safety concerns for affected buyers, and may cause financial losses on other compliant sellers too.

Malicious sellers could adopt various schemes to undermine consumers' interests. These schemes could occur: (i) before the transaction happens; (ii) during the transaction process; or (iii) after the transaction takes place. Before a transaction, some sellers may try reaching out to buyers through the IM functionality, offering buyers discounts and other benefits to trick them into conducting the transaction outside AliExpress, where we do not have the ability to detect frauds and scams. [*Confidential*].

As sellers on AliExpress compete for more exposure to potential buyers, which is affected by factors including the historical records of sellers' sales performance and the rating of their products and stores, sellers may also try to manipulate these data points in order to attract more buyer traffic. [*Confidential*].

There are also risks related to sellers attempting to seek access to the Platform by fraudulent means, in order to conduct activities that harm consumer interests or other fundamental rights. [*Confidential*]. Account takeovers enabled by hacking may cause financial losses for the victim due to further fraud risks.

Risks related to consumer protection can also occur through unresolved disputes between sellers and buyers on product or transaction-related issues, where either side may engage in harassing or stalking behaviour through the use of abusive language via IM and commenting services like product reviews.

While most risks related to consumer protection and fundamental rights emerge on the side of sellers, buyers may also abuse Platform functionalities to exploit promotional benefits. [*Confidential*].

AliExpress interactive games (such as "GogoMatch", "Merge Boss" and "Farm") and "Coins" are designed to encourage user loyalty and interactions on the Platform with rewards, for example through shopping coupons. While gamification is a common strategy across the industry to further engage and provide value to users, risks could emerge around behavioural addictions for users, including negatively affecting potential minors, who may have gained access to the Platform by evading our controls (in contravention of our Terms and Conditions).

AliExpress requires users to confirm during the registration process that they are over 18 and agree to our Terms & Conditions, however there is a risk that minors may nevertheless bypass this system. While there are prompts for visualising sensitive content and extensive moderation of prohibited items, the Platform still hosts potentially inappropriate for minors but compliant products, such as adult toys, sexual costumes, and sexual content.

b. Risks from Other Factors of the Platform (in line with Article 34(2) of the DSA)

Both in Year 1 and Year 2, we have assessed how the factors listed in Article 34(2) of the DSA may influence IPR risks:

- **Advertising systems and data practices**: There is an inherent risk that fraudulent sellers create unrealistic promotion schemes with prices much lower than the regular market value to drive up views on their advertisements. Furthermore, the advertisement customisation features developed by the Platform allow sellers to target certain buyer groups (albeit not in a precise manner). This could potentially trigger risks to consumer rights protection, as it may exclude certain buyers from equally accessing benefits provided by sellers in marketing campaigns, even if these benefits are still available to them upon proactive searching. While it is not possible to assess the full scale of these risks, the historical volume of detected infringements can serve as a proxy for this particular risk. Among the 2,764,070 product listings removed by the Platform due to fraudulent advertising campaigns in the time period from 1 July 2023 to 30 June 2024, 399,303 ([*Confidential*]) infringing product listings were advertised.
- **Recommender system:** The recommender system on the Platform is tuned to buyers' behaviour patterns, which include their clicks, likes, and purchase history. Some sellers may resort to unfair tactics in an attempt to boost their exposure in the Platform's recommender system by manipulating relevant data points. [*Confidential*].
- **Relevant policies and their enforcement:** Rules and policies published by AliExpress may not cover all types of scenarios of potentially fraudulent behaviour by users, thereby affecting our ability to take disciplinary action against such users to protect consumer interests and related fundamental rights.

- **Content moderation systems:** Even though the content moderation system serves to mitigate risks to consumer rights and other related fundamental rights, flaws in its functioning can also contribute to these risks. For instance, inaccurate screening of suspicious products, content, or accounts by algorithms may lead to unfair penalties against users. Taking the enforcement of sellers for IPR infringement as an example, between 1 July 2023 and 30 June 2024, out of a total of 2,764,070 appeals received, there were 28,556 (1.03%) successful appeals against our enforcement for IPR infringements.

Given that AliExpress operates as a marketplace, the potential theoretical risk—assuming no controls are in place—of violations of consumer rights and other related fundamental rights is "High". While it is not possible to measure the risk without any controls in place, this risk can be estimated by considering the following proxies. Between 1 July 2023 and 30 June 2024:

- We closed 297 fraudulent stores [*Confidential*].
- The number of EU buyers who did not get refunds through disputes associated with fraudulent sellers was 26,562, [*Confidential*].
- We received 7,279 reports of suspicious account takeover cases.

III. Existing Mitigations

In Year 2, we continued operating strong control mechanisms and further enhanced our consumer protection controls through our Year 1 mitigation commitments. The measures to manage risks related to Consumer protection and related fundamental rights can be grouped into several key areas: the tools developed for proactive risk mitigation, the task force and its management, internal and external risk identification methods, and the relevant risk mitigation workflows.

a. Transaction Specific Controls

AliExpress has developed a comprehensive risk-control framework that covers risks emerging from pre-transaction stage to after-transaction stage. Automatic keyword detection has been applied in the IM feature. Personal contact information and blacklisted keywords will be immediately blocked in order to prevent guided off-Platform transactions for non-compliant products, as well as to prevent malicious harassment and online stalking.

During the transaction, the Platform also has proactive measures to detect abnormal surges of order amounts or delivery declaration, as well as mechanisms to detect invalid order details or logistics details entered into the system. To further safeguard the transaction process, we also work with payment service providers to prevent theft of cards and other payment methods and to prevent leakage of payment channel information.

After the completion of a transaction, we will monitor for any user report of delivery or product quality issues, including keeping a record of "Not Received" rates and "Send Not As Described" rates for each seller. We also set up proactive reminders for buyers to report potential infringement of their

consumer rights, and provide them with easily accessible return and refund options. For example, in cases of the ordered product failing to be delivered within the promised time period, we will proactively send a notification to the user, and we will advise the user to initiate a dispute if necessary. When more severe situations occur, such as confirmed frauds and scams or sales of dangerous illegal products, the Platform will initiate proactive closure or confirmed fraudulent transactions, and follow local authorities' requirements regarding product recalls.

As an online marketplace, AliExpress has always stressed the need for quality control of products sold on the Platform. In addition to mitigation measures addressed in the P&C Products module, we have also developed pertinent measures to prevent products of inferior quality from being listed on the Platform in order to safeguard consumers' interests. For example, we implement monitoring and quality control measures (such as by identifying products with insufficient or misleading product information) and conduct thorough analysis of the price composition factors of individual products to detect misleading pricing. We also establish strict guidelines for the title, category, attribute parameters and detailed product descriptions to control for misleading or insufficient product descriptions.

b. Account Related Controls

We also adopt targeted measures to protect sellers registered on the Platform. AliExpress proactively identifies and intercepts attempts from high-risk buyer accounts, determined by scanning for bot behaviour, abnormal device information and IPs, that are more likely to unfairly claim vouchers and exploit other promotional benefits Further, to enhance its detection against fraud, AliExpress maintains credit profiles of sellers who have been previously detected as having participated in manipulating product reviews as well as for buyers who have been previously detected as having abused the interactive game features built into the Platform for user rewards.

For more severe risks identified above such as re-entry attempts from blacklisted sellers, account takeovers, and recidivism of deceptive behaviours from sellers, we operate a tracking system for these accounts, as well as a database of fraudulent account holder information. Thanks to this tracking system, we are able to impose enforcement actions against recidivist accounts effectively.

c. Vulnerable Population Related Controls

For vulnerable population groups, we set up special measures to protect them on the Platform. Regarding people with disabilities, AliExpress follows the Web Content Accessibility Guidelines in the Platform design, which allows users to enter the accessibility mode by selecting the help directory on the website homepage or turning on the accessibility mode in the mobile's device's setting when using the mobile application.

d. Protection of Minors

As stipulated in our Terms and Conditions, we do not provide services to minors (Individuals under the age of 18), and have specific restrictions on account registration and the use of payment methods.

When registering an account, users are clearly reminded that they must be 18 years or older. Additionally, the requirement for valid payment methods acts as a further control mechanism. When users attempt to make a purchase, they must provide a valid credit card or another accepted payment method, which typically requires the user to be 18 years or older. This requirement helps mitigate the risk of minors completing transactions on our platform. In addition to our controls on minors creating accounts on AliExpress, we currently have two types of age-restricted visibility mechanisms to mitigate the risk of users (including potential minors) encountering sensitive products such as adult products when accessing the Platform as a guest (i.e., without an account). Specifically, the Platform has the following features:

- **Age-verification mechanism***:* The age-verification mechanism appears as a pop-up window prompting confirmation that the user is over 18 years old when their search information or search terms relate to certain product categories (e.g., adult products); and
- **Adult products blurring control mechanism for browsing***:* Adult product listings (including, but not limited to, adult sex products etc.) will appear blurred first, until the user confirms they want to see them. As our policies do not allow minors on the service, this control is for all users. However, the control can protect minors should they access the service by bypassing our controls or should they be exposed to platform content if their parents or legal guardians are browsing the Platform in the company of a minor.

The above are additional control capabilities for protecting minors. These are without prejudice to the Platform rules which already restrict pornographic or other explicit or inappropriate content.

Additionally, we established and have maintained a SOP allowing parents to report cases of underage use. If a parent requests, or if the Platform confirms that a user is a minor, the user's account will be frozen. From 4 September 2023 to 30 June 2024, AliExpress received one DSR from parents based in the EU, and the concerned account had been thus successfully deleted following verification with the parents.

e. Interactive Games

The Platform has implemented comprehensive anti-fraud strategies for interactive games. Each time a user initiates a request in an interactive game (such as entering a game, completing tasks, or claiming rewards), the system intercepts users flagged as high risk. This strategy includes identifying users based on machine traffic, devices, IP addresses, and other mediums. If suspicious activity is detected, the Platform will block the user's current request to participate in the interactive game. This measure aims to prevent the mass claiming of platform benefits by malicious entities, thereby ensuring that legitimate users have fair access to the Platform's resources and protecting their rights.

The AliExpress Interactive Game Management Guidelines have been established in light of requirements regarding interactive game policies and regulations across countries. These guidelines aim to ensure the compliance of AliExpress' interactive games, and make sure that games undergo compliance and user experience evaluations before launch, modification, or removal. The Guidelines include two major requirements as governance controls:

- Any game must be approved by the legal and other relevant teams;

- The global Terms and Conditions (T&C) must be localised to ensure compliance within each relevant regional market or national market where applicable.

We also track the amount of time users spend on AliExpress' interactive games to understand the potential link to promoting addiction and monitor that the percentage of users spending significant time on such games remain below certain thresholds.

f. Advertising Systems and Data Practices

Since advertisements on the Platform are distributed using algorithms, there is a risk of unequal exposure for sellers participating in the Platform's targeted advertising programmes. To address this, we have implemented specific checks to prevent algorithmic discrimination within the advertising systems. Relevant sellers can choose between two advertising modes: "System-Intelligently Placed Ads" and "Custom Placed Ads." In the first mode, sellers specify the products to advertise, the countries or regions to target, and their campaign budget. However, neither the sellers nor the Platform can select specific buyer groups to target for seeing the ads. In the second mode, sellers can customise the buyer groups for their ads, but this customisation does not guarantee that the ads will be shown exclusively to the specified buyer groups.

We have also implemented a strict admission procedure for sellers to participate in the Platform's advertising programs, including but not limited to ensuring that sellers are not involved in dishonest operations, buyer fraud, or any other behaviour that harms buyer rights and interests. The Advertising pool is directly connected to the CRO department controls and the database of confirmed non-compliant products. Products targeted by the CRO department controls or labelled in that database will be automatically removed from the advertising pool, in order to safeguard users' experiences with the recommendation system on the Platform.

Given that the advertisement system on the Platform is powered by a recommender system, we established the Advertising Transparency Repository for the mandatory disclosure of advertisement information in compliance with the requirements in Article 39 (2) points (a) to (g) of the DSA. This Repository is publicly available and does not require user log-in. The Advertising Transparency Repository portal can be easily accessed through the "Tools" section and the "DSA-related Information" section of our site, which can both be accessed through the "Transparency Centre" located at the bottom of the interface of the AliExpress homepage. Since the establishment of the Repository, AliExpress has been continuously improving its accessibility. On 16 May 2024, AliExpress added an access point to the API in the Advertising Transparency Repository portal, along with API guidelines and FAQs that further help users understand how to use the search query tool as well as the API.

g. Recommender System

Along with the Recommendation system controls laid out in Section VI, the following are filtered from the recommendation pool to ensure that they will not appear as recommended items on the AliExpress Homepage: sexually suggestive content; adult products; potentially provoking or controversial content (e.g., products featuring skulls and blood); products featuring controlled drugs

(e.g., clothing with patterns of cannabis); and content or products with unverified IPR claims. Apart from non-compliant products and non-compliant content, we also limit the presence of poorly rated products on users' recommendation scenarios. The recommendation pool is directly connected to the CRO department controls and the database of confirmed non-compliant products. Products targeted by the CRO department controls or labelled in that database will be automatically removed from the recommendation pool, in order to safeguard users' experiences with the recommendation system on the Platform.

h. Relevant Policies and their Enforcement

We closely monitor developments in consumer protection laws within the European Union and its member states to ensure our terms and conditions address potential risk scenarios, emerging user trends, and align with relevant EU and member state legal requirements. As outlined in our Year 1 Report, AliExpress provides a number of detailed policies and rules regarding Consumer Protection. Our list of rules for P&C products include:

- AliExpress "Transaction but Not Selling" Rules;
- AliExpress "Guided Offline Trading" Rules;
- AliExpress "Disrupting Platform Order" Rules;
- AliExpress "Fake Shipment Rules";
- AliExpress "Mismatched Merchandise" Rules;
- AliExpress "Malicious Harassment Rules".

Violations of these policies may lead to the imposition of penalty points, following a similar approach as laid out in the Prohibited & Controlled Products section (See Section VII of the report).

i. Content Moderation Systems

For content moderation algorithms, we continuously monitor and adjust detection thresholds based on actual violations. These thresholds are iteratively improved using data from violations that were not detected by the algorithmic controls, thereby enhancing the algorithms' ability to identify non-compliant content and products.

Another area of focus is the prevention of fake ratings and reviews. AliExpress leverages big data analysis and artificial intelligence tools to detect abnormal patterns in reviews, such as timing anomalies or content similarities, and flag them as potentially fake. The Platform has also refined its rules to explicitly prohibit fake reviews and set clear enforcement actions for merchants who engage in this practice. This includes deducting points from merchant ratings, removing products from listings and, in severe cases, suspending or closing accounts. A reporting mechanism is also in place, enabling users to report suspicious reviews, which are promptly investigated by the Platform.

On the staffing side, we ensure the moderation team can handle tasks effectively by monitoring the timeliness of their work and adjusting shifts and staffing as needed. If task volume exceeds current

capacity, additional resources will be allocated. To maintain accuracy in manual reviews, we conduct random quality inspections. Moderators who fail to meet quality standards must retake qualification exams before continuing their duties.

As all content moderation operations take place on the AliExpress Risk Control System ([*Confidential*]), we have set up early warning mechanisms in place across all stages of making and enforcing a moderation decision. Regular risk inspection sampling is carried out to identify potential system failures, and any issues detected in the sampling will be promptly addressed by responsible personnel. Different types of risks (e.g., content, products, transactions, marketing) are completely separated in their moderation in the Risk Control system, which prevents system failures in one cluster of risk type interfering with other clusters, and improves the overall resilience of the system.

Given that there is always the risk of inaccurate moderation decisions being made, we provide users with easy-to-use appeal procedures to challenge moderation decisions. For EU-based sellers, if there is any doubt regarding the penalty received, sellers can seek assistance from the Platform's customer service portal to appeal against the decision, in line with article 20 of the DSA. The seller should then provide the required materials within the prescribed time frame and the appeal case will be transferred to the CRO for re-examination. Currently, [*Confidential*] customer service representatives are dedicated to assisting EU-based sellers, providing responses in Spanish, French, Polish, and English.

j. New Mitigation Measures

In line with Year 1 commitments, we have, in the past twelve months, made significant improvements to the effectiveness of our mitigation measures. Notably:

- **Choice model:** In addition to the P&C and IPR risks that the Choice service mitigates as discussed in the earlier sections, Choice also promotes consumer protection as it can guarantee faster, safer, and more economic deliveries for consumers as compared to non-Choice products sold by other sellers. Also, Choice has a 90-day free return period for most products and buyers can also benefit from a faster and smoother after sale care process as buyers engage directly with customer service representatives from AliExpress on behalf of the sellers.
- **Updates to published platform rules:** We have launched the AliExpress "Product Review" Rules, available in both Chinese and English. In the latest update to the "Product Review" Rules, we have specifically addressed the issue of manipulating product reviews and ratings. The practice of offering “incentivised reviews” is now officially subject to content moderation, aiming to further reduce potentially falsified and manipulated reviews. Additionally, we have updated the AliExpress “Seller Shipping Management Standards” by introducing new assessment criteria. These include the seller’s 48-hour shipment rate (sellers are expected to ship the order within 48 hours after payment of the order being completed), order cancellation rate, and Not Received (“NR”) dispute rate. The goal is to improve the consumer shopping experience by ensuring that sellers ship orders on time and deliver products more quickly.
- **Strengthened fraudulent user identification:** We have enhanced our systems to better detect and prevent fraudulent user activities. The expansion of our database of recognised

fraudulent activities and the improved training of detection algorithms have led to more accurate identification of suspicious attempts. Additionally, the continuous updates to our blacklisted merchants' backflow prevention system, coupled with new detection tools, have improved our ability to identify fraudulent sellers trying to obtain legitimate seller accounts by refining our systems to more effectively filter out suspicious login activities.

- **Optimised customer reporting and dispute resolution tools:** In August 2024, we introduced new hotline services in Spain and France, expanded local language support hours, and integrated user feedback into our detection mechanisms to improve the customer experience and reduce the risk of unresolved disputes.
- **Expanded local language support:** In response to the needs of our global user base, we have extended the availability of local language support by implementing AI translation technology. Going live in September, this will allow our 24/7 English chat service to be translated into local languages, which supports translation to Spanish, Portuguese, Italian, Dutch, German, French, and Polish.
- **Enhanced detection of inauthentic activities:** We have further developed our capabilities to identify and mitigate the risks associated with fake accounts and fraudulent user reviews. [*Confidential*].
- **Continuous improvement to the detection and verification algorithms:** We remain committed to advancing our detection and verification technologies. In Year 2, we have developed more sophisticated recognition algorithms, particularly for detecting commonly sold counterfeited goods. We have also expanded our historical data analysis, allowing for more accurate identification of high-risk accounts. Stricter enforcement measures against repeat offenders, particularly in cases of fake shipments, have been implemented, to further deter fraudulent activities.
- **Enhanced protections regarding minors:** We have reinforced our safeguards by launching the adult products blurring control mechanism for browsing related products. Additionally, we established standardised procedures to freeze accounts upon confirmed parental requests, reducing the risk of unauthorised access by underage users.

IV. Residual Risk

Despite our best efforts to mitigate the risks to Consumer protection and related fundamental rights on the Platform through proactive and reactive measures, we cannot fully eliminate the risks entirely due to the dynamic nature of the risk landscape. Our efforts to mitigate risk are made more complex by the evolving strategies utilised by users to manipulate the transaction process. Consequently, it is evident that a certain level of residual risks persists on the Platform. Based on the inherent risk score and mitigation effectiveness score of this risk module, the residual risk score is qualified as Medium-High. Nonetheless, we continue to work towards minimising the risk of disseminating P&C Products through the Platform.

Inherent Risk	Mitigation Effectiveness Score	Residual Risks

Based on the probability and severity scores calculated using the DSA Risk Assessment Rating Methodology, the inherent risk score is assessed as "**High**", which indicates a high concern around the probability of risks occurring that may have the potential to cause significant negative impact to the users.	Overall, the mitigation implementations are effective and resulted in a decreased exposure of related risk on the Platform. The mitigation effectiveness score is calculated to be "**Moderate**" (66%), indicating a minor likelihood of a control failure.	Based on the inherent risk score and mitigation effectiveness score, the residual risk is "**Medium-High**" on the Platform, which indicates a moderately high level of concern around the likelihood and impact of risks arising to users on the Platform after mitigation measures have been applied.

V. Conclusion and Future Mitigations

In Year 2, the residual risk rating of "Medium-High" has increased from a "Medium" rating in Year 1. This change is due to our updated methodology assigning a higher severity score to this category, resulting in an elevated residual risk score. We highlight that this increase in residual risk occurred despite improvements to our mitigation effectiveness score from Year 1.

We will continue to build up from the residual risk mitigation roadmap committed to in Year 1, to address the residual risks. We plan on improving our mitigation measures against Consumer Protection risks in the following areas, to target potential insufficiencies identified in the Year 2 Risk Assessment:

- **Strengthening fraudulent user's identification:** We will enhance security by introducing a "Card Payment Order Verification" method and implementing the "Account Freeze" action to safeguard accounts that have been compromised.
- **Enhancing detection of fraudulent seller behaviour:** We plan to identify more fraudulent merchants by working with third-party logistics data providers thus gaining access to more comprehensive and higher-quality logistics data to detect and prevent suspicious activities more effectively.
- **Improving detection of malicious harassment by sellers:** We will increase our ability to recognise consumer abuse by expanding keyword recognition coverage, enabling us to better identify and address instances of harassment or insults from sellers.

XII. Conclusion

This report highlights the result of AliExpress' second DSA systemic risk assessment exercise, carried out in line with the obligations set forth in Articles 34 and 35 of the DSA. Building on the foundational work established in the first risk assessment, we have, in our Year 2 risk assessment, refined our approach, enabling us to build on the insights gained from our Year 1 assessment to more precisely map specific risks that may arise across the Platform and evaluate the effectiveness of the controls we have implemented.

For our Year 2 assessment, we diligently identified, analysed and assessed the systemic risks in the Union stemming from the design or functioning of our services and its related systems, including algorithmic systems, or from the use made of our services. As AliExpress operates within a dynamic and fast-paced risk landscape common to many global online marketplaces where the transactions, types of sellers and buyers are increasing in volume and diversity, we focused on the risks that are specific to our service and divided our analysis into five separate modules allowing us to take into account the severity and probability of these systemic risks arising on or through our Platform. We assessed how our Platform could be used to disseminate prohibited and controlled products, illegal content, IPR infringements as well as to produce negative effects on consumer and data protection among other fundamental rights.

We then assessed the strengths of our existing control measures, outlining improvements made in the past year, following the results of our Year 1 DSA risk assessment. Overall, the analysis shows the strength of our approach, which is evidenced by an overall reduction in residual risk levels compared to Year 1. Nevertheless, it is inevitable that some residual risk will remain on our Platform as we operate in a dynamic risk landscape. To ensure we continue to effectively monitor and mitigate these risks, we remain committed to improving our controls and have, in each section, detailed how we plan to take additional reasonable, proportionate and effective measures in the next year, tailored to the specific systemic risks we have identified in our Year 2 assessment.

We look forward to continuing to collaborate closely with the European Commission, external researchers, and civil society to ensure that AliExpress remains a safe, stable, and trustworthy environment for all our users.

Annex 1. Risk probability thresholds

Probability	Percentage	Description
Almost certain	X >= 0.6%	More than 6 in every 1,000 checked accounts/ content/ products/ orders are identified as non-compliant. The risk occurs frequently during the provision of our services.
Likely	0.4 =< X <0.6%	More than 4 and no more than 6 in every 1,000 checked pieces of content or products are identified as non-compliant. This risk occurs at a noticeable rate during the provision of our services.
Possible	0.3% =< X < 0.4%	More than 3 and no more than 4 in every 1,000 checked pieces of content or products are identified as non-compliant. We have noticed isolated cases of the risk during the provision of our services.
Unlikely	0.2% =< X< 0.3%	More than 2 and no more than 3 in every 1,000 checked pieces of content or products are identified as non-compliant. The risk rarely occurs during the provision of our services.
Very unlikely	X < 0.2%	No more than 2 in every 1,000 checked pieces of content or products are identified as non-compliant. This risk almost never occurs during the provision of our services.

Annex 2. Severity scores and relevant descriptions

Severity	Score	Description
Very High	5	There is a severe risk of harm to the population affected by this risk and the risk may impact most users on the Platform. The consequences of this risk could be severe, and the situation cannot be effectively restored to pre-risk levels.
High	4	There is a significant risk of harm to the population affected by this risk and the risk may impact a significant number of users on the Platform. The consequences of this risk could be difficult to recover from, but the situation can be controlled and restored to pre-risk levels with difficulty.
Medium	3	There is a moderate risk of harm to the population affected by this risk and the risk may impact a moderate number of users on the Platform. The consequences of the risk could take time to recover from, but the situation can be controlled and restored to pre-risk levels.
Low	2	There is a minor risk of harm to the population affected by this risk and the risk may impact a minor number of users on the Platform. The consequences of the risk could be easy to manage, and the situation can be restored to pre-risk levels.
Very Low	1	There is a negligible risk of harm to the population affected by this risk and the risk may impact on a negligible number of users on the Platform. The consequences of the risk could be negligible, and the situation can easily be restored to pre-risk levels.

Annex 3. Inherent risk matrix and description of scores

		Inherent Risk Score				
Probability	**Almost certain**	Medium	Med. High	Med. High	High	High
	Likely	Low Medium	Medium	Med. High	Med. High	High
	Possible	Low Medium	Low Medium	Medium	Med. High	Med. High
	Unlikely	Low	Low Medium	Low Medium	Medium	Med. High
	Very unlikely	Low	Low	Low Medium	Low Medium	Medium
		Very low	**Low**	**Medium**	**High**	**Very high**
		Severity				

Inherent Risk	Description
High	Indicates a high probability of occurrence and significant negative impact to the users, such as a higher volume of affected users, large economic loss, serious physical health damage, etc.
Med High	Indicates a relatively high probability of occurrence and obvious negative impact to the users, such as a relatively higher volume of affected users, relatively serious economic loss, obvious physical health damage, etc.
Medium	Indicates the risk occurs sometime during the provision of the service and could result in moderate cause of bodily or psychological damage, etc.
Low Medium	Indicates that the occurrence is rare, and the impact is possible to cause bodily or psychological damage, or change to standard of living.
Low	Indicates that the occurrence is very rare, and the impact is unlikely to cause bodily or psychological damage, change to standard of living.

Annex 4. Mitigation effectiveness scores and relevant descriptions

For the Year 2 Mitigation effectiveness assessment questionnaire, we have adopted the mitigation maturity assessment as developed in the DTSP Maturity Rating Scale. The scale was implemented as follows:

Maturity Scale	Definition of Maturity Rating
Ad-hoc	Execution of mitigation measures are incomplete, informal, and inconsistent. Processes are not defined, not repeatable, and should be improved.
Repeatable	Execution of mitigation measures do not have standardised processes in places. There is some observability on how the measure works. There is scope of improving and formalising documentation practices.
Defined	Execution of mitigation measures entails processes that are defined and documented. Processes are more proactive than reactive and are implemented across the organisation.
Managed	Execution of mitigation measures entails processes that are defined, documented and managed through regular reviews. There is a set process for integrating feedback to mitigate process deficiencies.
Optimised	Execution of mitigation measures entails processes that are comprehensively defined and operating at the highest quality, with mature quality assurance in place. Processes are continuously improved to maximise the effectiveness of resources, maintain resilience and robustness.

Mitigation Effectiveness Rating	Range	Description
Very Strong	>=90%	Indicates that the mitigation measures are very well designed to mitigate the risk in its entirety. 90% or above of the questions in the questionnaire are answered positively.
Strong	70 <= X < 90%	Indicates minimal likelihood of a control failure. 70% to 90% of the questions in the questionnaire are answered positively.
Moderate	40 <= X < 70%	Indicates minor likelihood of a control failure. 40% to 70% questions in the questionnaire are answered positively.
Weak	10 <= X < 40%	Indicates that the mitigation measures are not properly designed to mitigate the risk in its entirety. 10% to 40% of the questions in the questionnaire are answered positively.

Very weak	X <= 10%	Indicates that the mitigation measures are poorly designed to mitigate the risk in its entirety. Less than 10% of the questions in the questionnaire are answered positively.

Annex 5. Residual risk matrix and description of scores

		Residual Risk Score				
Mitigation Efficiency	**Very Weak**	Low	Low Med	Medium	Med. High	High
	Weak	Low	Low Med	Medium	Med. High	High
	Moderate	Low	Low	Low Med	Medium	Med. High
	Strong	Low	Low	Low	Low Med	Medium
	Very Strong	Low	Low	Low	Low	Low Med
		Low	**Low Med**	**Medium**	**Med High**	**High**
		Inherent Risk				

Residual Risk	Description
High	Indicates a high level of concern around the likelihood and impact of risks arising to users on the Platform after mitigation measures have been applied (such as a high volume of affected users, large economic loss, serious physical health damage, etc. that can happen with high probability during the provision of service).
Med. High	Indicates a moderately high level of concern around the likelihood and impact of risks arising to users on the Platform after mitigation measures have been applied (such as a relatively high volume of affected users, relatively serious economic loss, obvious physical health damage, etc. that can happen with relatively high probability during the provision of service).
Medium	Indicates a moderate level of concern around the likelihood and impact of risks arising to users on the Platform after mitigation measures have been applied (such as moderate cause of bodily or psychological damage, etc can sometimes happen during the provision of service).
Low Med	Indicates a moderately low level of concern around the likelihood or impact of risks arising to users on the Platform after mitigation measures have been applied (such as possible impact to cause bodily or psychological damage, or change to standard of living but the risk occurrence is rare during the provision of service).
Low	Indicates a low level of concern around the likelihood or impact of risks arising to users on the Platform after mitigation measures have been applied (such as impact is unlikely to cause bodily or psychological damage, change to standard of living and the risk occurrence is very rare during the provision of service).

Annex 6. EU Watch List submission

[Please refer to the separate stand-along document]