Deloitte.

*Together makes progress*

CENTRE *for*
REGULATORY
STRATEGY
EMEA

# The online marketplace and e-commerce agenda

## How to stay ahead of the regulatory curve

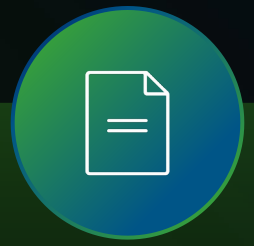
June 2026

# The structure of this report

Click on the icons to navigate to each section

## EXECUTIVE SUMMARY

*Page 3*



- Operators of online marketplaces and e-commerce sites are subject to a **fast-moving regulatory environment across the UK and EU**.
- This section summarises **eight priority areas** which, in our view, can help companies keep pace with evolving regulatory expectations.

## HOW COMPANIES CAN RESPOND

*Page 4 - 16*

- **This section deep dives into each of the eight priority areas** we have identified, referencing the most relevant regulatory requirements and how companies can respond.
- Fictional **case studies** bring three of these priority areas to life, illustrating practical implications for the customer journey, minors' protection and AI governance.

## ANNEX

*Page 17 - 21*

- This section sets out a **taxonomy** of the e-commerce and online marketplace ecosystem, along with the **features of an online marketplace** that may trigger regulatory obligations.
- **We also set out a legal and regulatory glossary** relevant to the content of this report.
- Finally, we list the **report authors** and **contacts** for a follow-up conversation.

© 2026 Deloitte LLP. All rights reserved.

# Executive Summary

## Navigating regulatory priorities for online marketplaces

### The increasing regulatory challenge

Online marketplaces are subject to requirements across online safety, consumer protection and AI regulation, alongside wider obligations spanning financial crime, product safety, trade and sustainability.

In addition, a regulatory emphasis on how marketplaces are designed, operated and governed means there is an increased focus on user journeys, risk assessment methodologies, transparency and AI-enabled systems.

Marketplaces that take a proactive, joined-up response will be better placed to enhance trust, reduce risk, realise operational efficiencies and support sustainable growth.

There is no formula for compliance, with the exact response differing on a company-to-company basis. However, in this fast-moving and complex environment, this report sets out our view on eight priority areas that online marketplaces can prioritise to stay ahead of the regulatory curve.

### Who is this report for?

This report is intended for senior leaders across legal, compliance, risk, strategy, product, technology and operations functions.

Whilst it is most relevant to marketplaces hosting third-party sellers, many themes also apply to broader e-commerce models, including own-brand web stores, retailers and discovery or comparison services.

### Eight priority areas to guide a response

1. **Risk assessments as the backbone of compliance:**
   Risk assessments are the prism through which platforms are expected to identify risk and mitigate harm, with rising expectations on quality and evidence. As requirements span multiple regimes, marketplaces should prioritise a consistent, scalable methodology.

2. **Ensuring a fair customer journey:**
   Regulators are scrutinising how platform design shapes user outcomes across pricing, ranking, reviews, subscriptions and AI-driven personalisation. Marketplaces should review design decisions to ensure they are transparent, fair and defensible through clear supporting evidence.

3. **Protecting minors by design:**
   The protection of minors is a clear regulatory priority, requiring platforms to assess risks and implement safeguards across the entire user journey. This may include restricting access to age-inappropriate products and high-risk features (e.g. addictive functionalities) and applying controls across recommendations and advertisements. Safeguards should be underpinned by effective age assurance.

4. **Mitigating financial crime risks:**
   Marketplaces face exposure both as a vehicle for, and a victim of, financial crime. An effective response requires controls across onboarding, listings and transactions, including strong identity verification, monitoring of platform activity, and user/third-party reporting mechanisms.

5. **Transparency as a core regulatory expectation:**
   Regulators expect transparency in relation to trader information, advertising, recommendations and platform decisions. Marketplaces should prioritise providing clear, accurate and explainable information to users, whilst being ready to evidence decisions to regulators.

6. **Responsible AI governance:**
   As AI is deployed across the marketplace value chain, specific use cases (e.g. chatbots) may fall within scope of regulatory requirements. Marketplaces should map use cases against requirements and implement proportionate governance and controls.

7. **Enhanced cross-border oversight:**
   Greater regulatory oversight of cross-border e-commerce means that marketplaces are taking on greater compliance responsibility for how goods enter and move across different jurisdictions. This requires strong seller and product governance and effective customs data capabilities.

8. **Scale as a regulatory trigger:**
   As marketplaces grow, regulatory expectations can increase. Marketplaces should monitor growth against thresholds and ensure preparedness, for example through a readiness roadmap.

© 2026 Deloitte LLP. All rights reserved.

# How companies can respond

Deep dive into the eight priority areas for action, outlining how online marketplaces can respond to evolving UK and EU regulatory requirements. Fictional case studies bring three of these priority areas to life, illustrating practical implications for the customer journey, minors' protection and AI governance.

© 2026 Deloitte LLP. All rights reserved.

# The regulatory landscape

## Key regulatory domains relevant to online marketplaces

Online marketplaces face a wide range of regulatory requirements that shape how they design, govern and operate their platforms, from user interaction and product discovery to trader oversight, pricing and the use of AI-enabled tools. Here, we introduce the main regulatory domains that online marketplaces should have on their radar. We use the icons below throughout this section to highlight which of these regulatory domains apply to each of the eight priority areas that we have identified.

### ONLINE SAFETY

Requirements to assess and mitigate risks, with an emphasis on illegal content, protections for minors, and stronger obligations for larger or high-risk services.

### CONSUMER FAIRNESS

Focus on fair and transparent pricing, reviews, and subscription flows, with growing scrutiny of manipulative or addictive design and unfair practices.

### AI

AI scrutiny is increasing, with a focus on high-risk use cases, transparency and how businesses deploy or rely on AI tools.

### FINANCIAL CRIME

Multiple regulatory domains are relevant to marketplaces, including fraud, money laundering, terrorist financing, sanctions, tax evasion, bribery and corruption.

### PRODUCT SAFETY

Increasing marketplace accountability to monitor listings, restrict unsafe goods and remove harmful products.

### TRADE

Growth in cross-border e-commerce is reshaping how regulators approach customs and trade, driving more data-driven, digitised and platform-centric oversight.

### SUSTAINABILITY

Requirements around product sustainability and transparency, packaging and waste management, and human rights and environmental risks across value chains.

**These icons are used to map relevant regulatory domains across each of the eight priority areas that follow.**

© 2026 Deloitte LLP. All rights reserved.

# 1. Risk assessments as the backbone of compliance

## Use a consistent, scalable risk assessment methodology to identify risks and mitigations

Risk assessments are the prism through which platforms are expected to identify risk and mitigate harm, with rising expectations on quality and evidence. As requirements span multiple regimes, marketplaces should prioritise a consistent, scalable methodology.

### Regulatory areas

**Online safety:** In the UK, marketplaces must complete and maintain risk assessments on illegal content and risks to children, with additional obligations for larger 'categorised' services. In the EU, all platforms accessible to minors should conduct a 'risk review', whilst the largest platforms must conduct a systemic risk assessment.

**AI:** Risk management, monitoring and accountability are core requirements of the EU AI Act, particularly for high-risk use cases, with expectations to update assessments over time.

### Key Considerations

- **Assess risks across the full value chain and key user journeys.** Rather than looking through the lens of individual regimes, consider risks across each stage of the value chain, including how risks may differ for different user groups and journeys.
- **Focus on marketplace-specific risk exposure.** Prioritise risks such as illegal or unsafe goods, minors' access to age-inappropriate products or features, repeat bad actors, fraud, and AI-driven moderation or ranking decisions.
- **Develop a consistent, scalable assessment methodology.** A common framework applied and adapted to specific regulations can reduce duplication, improve consistency in messaging, and support clearer regulatory engagement.
- **Ground assessments in robust and consistent evidence.** Leverage common data sources across risk assessments (e.g. complaints, user reports and external sources) to enhance credibility and repeatability.
- **Embed cross-functional ownership and governance.** Input from across product, operations and other business areas is critical to accurately reflect how risks arise in practice.
- **Continuously update assessments as products and features evolve.** Refresh assessments ahead of material changes to design or operation to ensure risks are identified and mitigated early.
- **Consider adopting established principles and recognised frameworks.** Doing so can enable consistency and demonstrate credibility with regulators. Examples include UN Guiding Principles, ISO 31000 and the DTSP Best Practice Framework.

### Regulatory expectations for risk assessments

**The bar is rising on both quality and process**

- In the UK, under the Online Safety Act (OSA) Ofcom has signalled it expects clearer risk-level explanations, stronger evidence, more robust analysis of platform features and functionalities, alongside demonstrable control effectiveness and governance.
- In the EU, systemic risk assessments are central to ensuring a fit-for-purpose approach under the Digital Services Act (DSA). Investigations to date demonstrate a focus on how platforms identify illegal product risks, the effectiveness of moderation, and the resources allocated to mitigation. Recent enforcement action by the European Commission has only reinforced the pivotal role that risk assessments play in this respect.

**Assess new features proactively and consider incremental risk**

- Platforms are expected to assess risks associated with new or updated features before launch and update risk assessments accordingly.
- Assessments should clearly evidence incremental risk, including whether changes alter the platform's risk profile or trigger additional regulatory obligations (e.g. specific measures under Ofcom's Codes of Practice in the UK).
- Marketplaces should identify proportionate mitigations and demonstrate that these are effective in managing new risks.

© 2026 Deloitte LLP. All rights reserved.

# 2. Ensuring a fair customer journey

## Review design decisions and ensure they are transparent, fair and defensible

Regulators are scrutinising how platform design shapes user outcomes, across pricing, ranking, reviews, subscriptions and AI-driven personalisation. Marketplaces should review design decisions to ensure they are transparent, fair and defensible through clear supporting evidence.

### Regulatory areas

**Consumer fairness:** Greater scrutiny of pricing, reviews, subscriptions and cancellation journeys, requiring evidence of fair design choices.

**Online safety:** Focus on design, recommendations and features that may be addictive or amplify harm, particularly for minors. Very Large Online Platforms (VLOPs) face additional requirements in the EU.

**AI:** Tighter expectations for AI-enabled features, with prohibited practices under the EU AI Act including the use of harmful manipulative or deceptive techniques, and exploitation of vulnerabilities.

### Key Considerations

- **Prioritise high-impact journeys where design shapes user outcomes.** Points where small design choices materially influence decisions, including discovery, product pages, checkout and subscription processes, may face particular regulatory scrutiny.
- **Make key information clearly available before commitment.** Ensure total price, mandatory charges, sponsored placement, seller information and subscription terms are consistently clear and visible at relevant points in the transaction journey.
- **Avoid unfair pressure or hidden friction.** Identify and rectify any bad practices, which may include misleading urgency claims, repeated prompts, pre-selected options, unclear opt-outs, or cancellation routes that are harder than sign-up.
- **Assess safety, vulnerability and addictive design risks.** Review recommendations, notifications, rewards and engagement features to ensure they do not expose minors or vulnerable users to harm or drive unsafe or inappropriate behaviours.
- **Strengthen governance of reviews.** Competition and Markets Authority (CMA) guidance in UK highlights publication of a policy prohibiting fake, misleading or undisclosed incentivised reviews, along with an assessment of review-related risks and maintenance of proportionate controls.
- **Govern AI-enabled personalisation.** Apply controls to ranking algorithms and promotions to mitigate the risk of manipulation/exploitation. Ensure recommender system transparency (see *page 13*), whilst VLOPs must also offer a non-profiling option in the EU.
- **Ensure high-impact design choices are well governed and defensible.** Apply robust governance processes and maintain clear documentation outlining the rationale for defaults, ranking, pricing presentation, retention journeys as well as results from A/B testing, ensuring future explainability.

### Features likely to attract regulatory scrutiny

**Search / discovery**

- Sponsored placements not clearly labelled
- Preferential prominence for certain sellers or products

**Product page**

- Ads, promotions or commercial links not clearly disclosed
- Fake or misleading reviews without adequate controls

**Checkout**

- Mandatory charges not set out in the headline price
- Default add-ons or pre-selected extras

**Subscription / membership / seller plans**

- Easier to sign-up/upgrade than to cancel/downgrade
- Undue friction when stopping automatic renewal or requesting a refund

**Personalisation / AI-driven promotion / engagement**

- Recommendations steering minors or vulnerable users towards high-risk products
- Nudges or features encouraging excessive browsing or spending (e.g. infinite scrolling, push notifications, rewards for engagement)

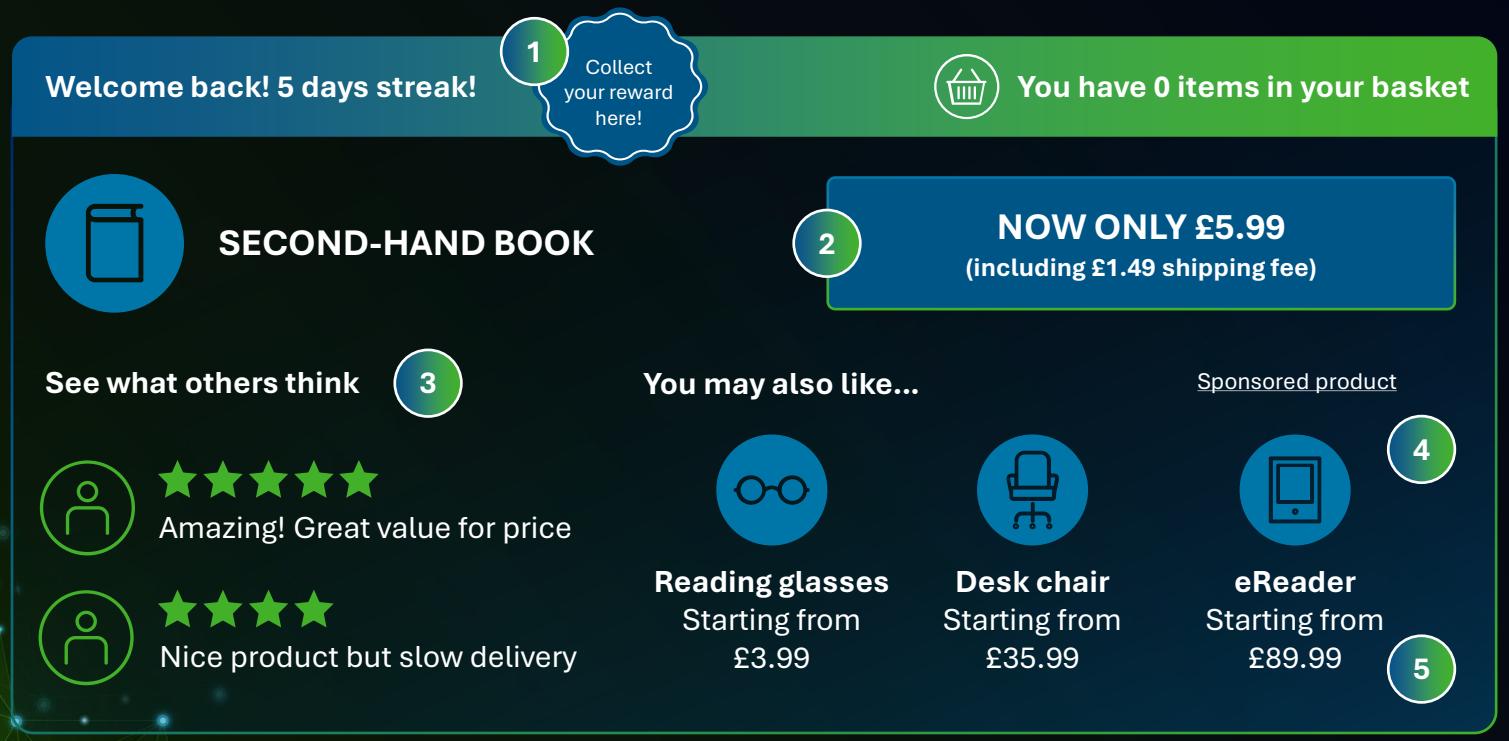
© 2026 Deloitte LLP. All rights reserved.

# Case study: developing a fair and compliant user journey

## e-Shopentra, a fictional online marketplace allowing third-party sellers

This case study illustrates how a fictional online marketplace reviews its end-to-end user journey to ensure alignment with regulatory expectations on reviews, transparency, choice architecture and addictive design. It highlights the importance of developing a demonstrably fair, transparent user journey and interface, supported by clear evidence.

- **Service:** e-Shopentra is a fictional online marketplace operating in the UK and EU. The platform allows third-party sellers to list products, advertise promotions and collect customer reviews. It also uses personalised recommendations, push notifications, loyalty rewards and time-limited offers to drive engagement and repeat purchases.
- **Status:** e-Shopentra is reviewing its customer journey following increased regulatory scrutiny of fake reviews, pricing transparency, paid promotions, manipulative design and features that may encourage excessive engagement. The company wants to ensure that reviews are reliable, paid content is clearly disclosed, and engagement features are proportionate, transparent and supported by evidence.




### Actions that e-Shopentra should take

1. **Controls over addictive design:** Engagement features such as push notifications, rewards, streaks, infinite scroll and personalised recommendations should be assessed for potential harm, including excessive browsing, repeat spending or exposure to unsuitable products. This is likely to attract particular scrutiny where these features are accessible to minors.
2. **Pricing transparency:** Any additional fees, taxes, or any other charges must be disclosed upfront. For this reason, e-Shopentra clearly includes the shipping fee in the total price, so that buyers can make informed purchasing decisions. e-Shopentra should ensure it does the same across all product pages.
3. **Review integrity:** e-Shopentra should develop a publicly accessible policy prohibiting fake reviews and setting out its approach to incentivised reviews. It should also conduct recurring risk assessments and take proactive action to minimise risks (e.g. a clear process to detect, investigate and remove prohibited reviews).
4. **Disclosure of incentives:** Buyers should be able to understand when search results, rankings, or reviews are influenced by sponsorship, seller status, or commercial incentives. Here, e-Shopentra clearly labels a sponsored product and does not present it as a purely organic result. It should ensure this is applied across its marketplace.
5. **Evidence and accountability:** Across the user journey, e-Shopentra should ensure high-impact design choices are documented, tested and subject to appropriate governance. e-Shopentra should be able to explain the rationale for review presentation, ranking, notification frequency and promotional mechanics.

© 2026 Deloitte LLP. All rights reserved.

# 3. Protecting minors by design

## Apply safeguards to products and features accessible to minors, underpinned by effective age assurance

The protection of minors is a clear regulatory priority, requiring platforms to assess risks and implement safeguards across the entire user journey. This may include restricting access to age-inappropriate products and high-risk features (e.g. addictive functionalities) and applying controls across recommendations and advertising. Safeguards should be underpinned by effective age assurance.

### Regulatory areas

**Online safety:** The OSA and DSA require platforms accessible to minors to assess risks and implement child-specific safeguards, with age assurance a key enforcement priority.

**Consumer fairness:** Increased scrutiny of design features (e.g. recommender systems, engagement functionalities) that may exploit minors' vulnerabilities or drive harmful behaviours.

**Product safety:** Marketplaces may be responsible for preventing minors from accessing unsafe or age-restricted products sold by third-party sellers.

### Key Considerations

- **Set and enforce a clear minimum age policy.** Regulators increasingly expect platforms to enforce minimum age policies. If age restrictions are not effectively enforced, regulators will treat the service as accessible to minors regardless of stated T&Cs.
- **Consider whether minors can access the service in practice.** Minors may still access services (e.g. via guest browsing) even where age assurance is required for account creation.
- **Where minors can access the service, implement proportionate safeguards.** Conduct risk assessments (see *page 6*) and apply age restrictions aligned to the level of risk across products, features (e.g. livestreaming) and user journeys.
- **Enforce age-restrictions through proportionate age assurance.** Higher-risk use cases (e.g. age-restricted products) or enforcing an 18+ minimum age may require stronger verification, balanced against privacy and accessibility considerations.
- **Ensure a compliant age assurance approach.** Ensure approaches align with criteria relevant to the jurisdiction in question, e.g. the European Commission or Ofcom. In the EU, consider integrating with emerging EU Digital Identity Wallets to align with data minimisation expectations.
- **Protect minors from harmful or inappropriate commercial practices.** Clearly label ads and influencer marketing, do not present ads to minors based on profiling, and provide appropriate controls over product feeds and recommendations.
- **Do not expose minors to AI-driven commercial nudging.** Avoid systems that influence or steer minors' financial decisions, such as purchases, particularly through conversational formats (e.g. chatbots).
- **Avoid addictive and manipulative design features.** Avoid minor exposure to design features that can lead to excessive, impulsive, unwanted spending or addictive behaviours (e.g. gamified incentives or urgency claims).

### Features likely to attract regulatory scrutiny

**Entry and access**
- Weak or unenforced minimum age policies
- Guest browsing without proportionate safeguards
- Account creation without appropriate age assurance

**Discovery, recommendations and features**
- Product feeds exposing minors to age-restricted or unsuitable products
- Recommender systems promoting high-risk products, content or features
- High-risk features accessible to minors (e.g. livestream shopping features enabling interaction with other users)

**Advertising and promotions**
- Paid placements or influencer-style marketing that are not clearly labelled
- Targeted adverts based on minors' personal data
- Promotions that exploit minors' limited commercial literacy

**Marketplace design / Checkout**
- Urgency claims, rewards or gamified incentives encouraging impulsive purchases
- Checkout journeys that allow age-restricted purchases without effective checks
- Defaults or nudges increasing exposure to inappropriate products or features

© 2026 Deloitte LLP. All rights reserved.

# Case study: ensuring proportionate safeguards to protect minors

## Social Mercato, the online marketplace of a fictional social media company

This case study illustrates how a fictional social media platform considers enhancing protections for minors on its marketplace service. It highlights key considerations for preventing minors from accessing age-restricted products and high-risk features, while meeting expectations under the UK OSA and EU DSA.

- **Service:** Social Mercato is the online marketplace of a fictional social media company operating in the UK and the EU. It supports product listings by third-party sellers, reviews, seller Q&A, personalised recommendations and in-app messaging between buyers and sellers. Some sellers list **adult-only products**, including alcohol, vapes and bladed items. Recently, Social Mercato launched a **livestream shopping feature**, enabling real-time product demonstrations, time-limited discounts and interactions with viewers.
- **Status:** Social Mercato has determined that minors are likely to access the service and is reviewing its controls to ensure compliance with child protection duties. In particular, it wants to ensure that minors cannot purchase age-restricted products and are not exposed to harmful content and interactions.

### 1 T&Cs

- Users must be 18+ to open an account on Social Mercato
- Wider social media account age limit is set at 13

### 2 ENTRY & ACCOUNT

- No effective enforcement of the minimum age to create an account

### 3 PRODUCT DISCOVERY

- Safe search feature and no nudging towards age-restricted items during guest browsing

### 4 PURCHASING ADULT-ONLY ITEMS

- No age check for logged-in buyers
- Guest checkout feature

### 5 LIVESTREAM SHOPPING

- New feature launched in the UK and the EU

### Actions that Social Mercato should take

1. **Terms & conditions:** T&Cs set a clear minimum user age at 18. Nonetheless, because no effective age assurance methods are used to enforce it, minors are likely to access the marketplace. Given this, Social Mercato should complete a regular OSA risk assessment and DSA risk review and introduce child-specific safety measures.
2. **Entry & account:** Social Mercato should implement appropriate age assurance measures to enforce its 18+ age policy. In the EU, for example, DSA guidelines specify that service providers which set a minimum age of 18 in their T&Cs are expected to use age verification methods to mitigate the risk of underage users accessing their service.
3. **Product discovery:** During guest browsing, the marketplace should be safe by default. For example, Social Mercato should consider hiding age-inappropriate content from search results, recommendations, and advertisements for logged-off users.
4. **Purchasing adult-only items:** Beyond verifying the age of users to enforce its 18+ minimum age policy, Social Mercato should verify the age of buyers during guest checkout for adult-only items.
5. **Livestream shopping:** Before introducing this new feature, Social Mercato should update its child-specific risk assessment and risk review. If the livestream feature is available on the broader social media platform, the company should also monitor potential new Ofcom requirements on the use of age assurance to limit actions on child-hosted livestreams.

© 2026 Deloitte LLP. All rights reserved.

# 4. Mitigating financial crime risks

## Prioritise robust controls, including identity verification and monitoring of transactions, listings and user activity

Marketplaces face exposure both as a vehicle for, and a victim of, financial crime. An effective response requires controls across onboarding, listings and transactions, including strong identity verification, monitoring of platform activity, and user/third-party reporting mechanisms.

### Regulatory areas

**Financial Crime:** Financial crime obligations, including fraud, money laundering, terrorist financing, sanctions, bribery and corruption, and tax evasion are highly relevant to online marketplaces, requiring risk-based governance, due diligence and effective controls.

**Online safety:** Specific financial crime risks are increasingly captured by online safety regimes, requiring marketplaces to assess and mitigate risks associated with fraudulent listings and broader illegal activity, alongside verifying key seller information.

### Key Considerations

- **Prepare for dual exposure as both a vehicle for, and a victim of, financial crime.** Marketplaces can be used to facilitate illicit activity while also facing direct loss, operational disruption, enforcement risk and reputational damage.
- **Prioritise robust onboarding and identity verification.** Not only is verifying key identity and contact information of sellers a key DSA requirement, strong onboarding and Know Your Customer controls can reduce wider risk exposure, including tax-related risks.
- **Monitor transactions, listings and user behaviour for coordinated abuse.** Marketplaces should prioritise detection of fake sales, scam listings, over/under-pricing, chargeback abuse and buyer–seller collusion used to move or conceal illicit value.
- **Empower users to report illegal activity.** Clear reporting tools can help marketplaces respond quickly to fraudulent listings and other illegal activity, including via DSA-mandated Notice and Action mechanisms.
- **Prioritise reports from designated trusted flaggers and equivalent expert bodies.** These reports may be of higher quality, more actionable and can enable faster identification and removal of fraudulent content in line with online safety requirements.
- **Layer and embed financial crime controls across the complete marketplace operating model.** Risks may arise across onboarding, search, listings, messaging, payments, fulfilment and refunds, and require coordinated, end-to-end mitigation.
- **Prioritise internal fraud risk management under the UK 'Failure to Prevent Fraud' offence.** Focus on reasonable fraud prevention procedures to prevent employees and associated persons committing fraud that benefits the organisation.
- **Adopt an intelligence-led and dynamic assessment of risks.** Leveraging horizon scanning and external insights enables marketplaces to continuously update controls in response to evolving threats and regulatory expectations.

### How financial crime risks arise in marketplaces

| Risk area | Platforms as a vehicle | Platforms as a victim |
|---|---|---|
| **Fraud** | Used to carry out scams, e.g. fraudulent listings, non-delivery fraud, fake goods, triangulation fraud or buyer–seller collusion. | Targeted through fake merchants, account takeover, refund abuse, coupon abuse or chargebacks, impacting trust and causing direct loss. |
| **Sanctions** | Used to access goods, payments or services in ways that may breach sanctions, including via sanctioned actors, restricted goods or transactions involving sanctioned actors or countries. | Exposed to regulatory, enforcement or reputational risk where due diligence and screening of users, third parties, goods, payments or destinations is ineffective (e.g. contracting with a sanctioned entity). |
| **Money laundering** | Used to move or disguise illicit value through fake sales, over/under-pricing, circular trading and chargeback abuse. | Exploited where weak onboarding or monitoring allows mule accounts, refund abuse or structured transactions to go undetected. |
| **Terrorist financing** | Used to transfer funds covertly through ordinary-looking purchases, listings, donations or repeated low-value transactions. | Exposed where controls fail to identify suspicious payment patterns (e.g. repeated small payments) or mule accounts. |
| **Tax evasion** | Sellers may under-report income, charge VAT but fail to remit it to tax authorities, misclassify goods (e.g. to access reduced VAT rates), issue false invoices or obscure cross-border sales activity. | Exposed where poor seller verification or limited transaction visibility weakens tax reporting, VAT controls or cooperation with tax authorities. |

© 2026 Deloitte LLP. All rights reserved.

# 5. Transparency as a core regulatory expectation

## Ensure information on traders, products, advertising and platform decisions is clear, accurate and explainable

Regulators expect transparency in relation to trader information, advertising, recommendations and platform decisions. Marketplaces should prioritise providing clear, accurate and explainable information to users, whilst being ready to evidence decisions to regulators.

### Regulatory areas

**Online safety (EU):** All platforms face a range of transparency requirements relevant to advertising and content moderation, with VLOPs facing further obligations. Marketplaces face further specific duties relating to trader traceability, interface design and consumer notifications where illegal products are sold.

**Online safety (UK):** Larger marketplaces may face additional transparency reporting and risk assessment publication duties under the OSA categorised services regime.

### Key Considerations

- **Ensure trader information is visible and reliable.** Buyers should be able to see key seller details (e.g. contact information and address) before transacting, supported by processes to verify and maintain accuracy.
- **Build compliance into product listing design.** Seller interfaces should require standardised product, safety and compliance information upfront, supported by proportionate pre- and post-listing checks.
- **Ensure effective buyer notification when illegal products are detected.** Ensure processes are in place to identify and contact affected buyers, and clearly communicate risks, seller details and redress options where relevant.
- **Ensure clear and real-time advertising transparency.** It should be immediately obvious when content is an advert, who is behind it, and why buyers are being targeted, supported by consistent labelling and (for VLOPs) public ad repositories.
- **Provide transparency and user control over recommendations.** Clearly explain the key factors driving rankings and recommendations and provide accessible tools for users to adjust or switch between available recommendation modes.
- **Build robust content moderation transparency reporting.** Ensure robust, repeatable processes are in place to support regular, structured reporting on moderation activity in line with DSA requirements, with enhanced obligations for VLOPs.
- **Develop flexible data capabilities for bespoke transparency requests.** The largest marketplaces should prepare for regulator-driven reporting under the OSA, including risk assessment disclosures and tailored transparency reporting.

### Regulatory expectations for transparency

**Clear**

- Information is easy for users to find before they make decisions
- Explanations are clear, timely and not buried in policies

**Accurate**

- Trader, product and advertising information is verified where required
- Processes keep information up to date and correct inaccuracies

**Explainable**

- Buyers can understand why they see adverts, rankings or recommendations
- Affected users receive clear reasons for platform decisions

**Traceable**

- Marketplaces can evidence how information was collected, checked and used
- Records support reporting, audit and regulator information requests

© 2026 Deloitte LLP. All rights reserved.

# 6. Responsible AI governance

## Map AI deployments against regulatory requirements and put appropriate controls and governance in place

As AI is deployed across the marketplace value chain, specific use cases (e.g. chatbots) may fall within scope of regulatory requirements. Marketplaces should map use cases against requirements and implement proportionate governance and controls.

### Regulatory areas

**AI:** The EU AI Act prohibits certain AI practices, alongside imposing stringent obligations on high-risk use cases and transparency obligations for certain user-facing systems. Requirements vary by role in the value chain and use case (e.g. recommender systems, content generation), requiring an assessment for each application.

**Online safety:** AI features (e.g. recommender systems, moderation tools, chatbots) should be assessed as part of UK and EU risk assessments. Platforms are expected to explain and justify certain AI-driven decisions (e.g. content moderation), including via DSA transparency reporting in the EU.

### Key Considerations

- **Map AI use cases against applicable regulatory requirements.** For example, requirements are more onerous where the AI system is developed in-house or where substantial modifications are made to a third-party AI system.
- **Assess AI features as part of the risk assessment process.** Evaluate recommender systems, chatbots and moderation tools within existing frameworks *(see page 6)*, including their impact on user risk.
- **Prepare for emerging risks from more autonomous AI systems.** For example, AI agents may enable a wider range of activity, increasing the risk of straying into a higher risk category or other regulated areas, requiring stronger oversight and safeguards.
- **Ensure transparency where users interact with AI systems.** Users should be clearly informed when they are interacting with AI, for example chatbots or interactive AI agents, unless this is already obvious.
- **Collaborate with sellers to ensure compliant use of AI.** Set clear policies and expectations (e.g. labelling AI-generated content) through T&Cs and seller guidance.
- **Consider leveraging AI as a compliance tool, with appropriate safeguards.** If using AI for moderation and detection, ensure accuracy, effectiveness and lack of bias (for example human oversight, as per Ofcom's proposed proactive technology criteria in the UK).
- **Ensure content moderation decisions are explained.** Even where AI is used in content moderation, users should receive clear reasons for decisions (a DSA 'Statement of Reasons' in the EU) and be able to understand and challenge outcomes where appropriate.
- **Capture evidence to demonstrate compliant AI outcomes.** Maintain evidence from testing and monitoring to demonstrate how systems operate and how risks are managed.

### Deploying an AI chatbot

*The table below sets out a number of different regulatory obligations that may apply to a customer-facing AI chatbot used to support product search by offering personalised recommendations.*

| Area | Selected regulatory implications |
|---|---|
| **Transparency** | To comply with incoming AI Act transparency requirements in the EU, inform users they are interacting with AI and clearly label AI-generated or manipulated media where relevant. |
| **High-risk systems** | In the EU, high-risk AI systems will face extensive requirements covering data quality and management, technical documentation, human oversight, and accuracy and robustness, amongst others.<br>This will apply only if the chatbot is used in specific high-risk contexts. For example, if the chatbot determines eligibility for Buy Now Pay Later options based on a creditworthiness assessment, this may bring it into scope. |
| **Online Safety** | Ensure the chatbot is considered as part of risk assessments under UK and EU online safety regimes, and that appropriate mitigations are implemented.<br>As a recommender system, under the DSA, the marketplace should ensure that the main parameters used to inform recommendations are set out in T&Cs, alongside any options for users to modify or influence these parameters. |

© 2026 Deloitte LLP. All rights reserved.

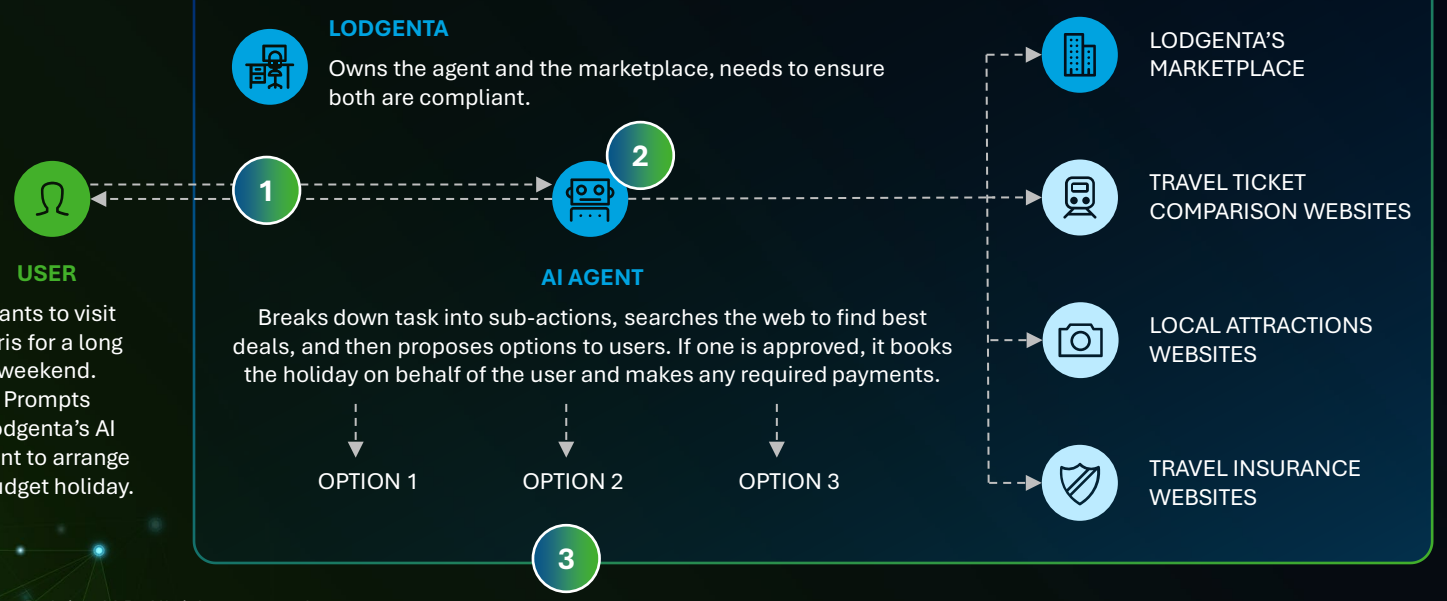
# Case study: governance of an AI chatbot and agent

## Lodgenta, a fictional online marketplace enabling users to advertise short-stay holiday accommodation

This case study illustrates some of the regulatory considerations a fictional marketplace specialised in short-stay holiday accommodation should consider before deploying an AI agent capable of designing and pre-packaging a full holiday experience for its users.

- **Service:** Lodgenta is a fictional large marketplace which allows sellers to advertise short-stay holiday accommodation (e.g. hotels, resorts, apartments) across the UK and EU. Lodgenta plans to expand its business model to provide its buyers with an end-to-end user journey comparable to a travel agency but at much lower prices.
- **Status:** Lodgenta is planning to introduce an AI agent based on a third-party AI model. Customers would be able to prompt its agent with a task (e.g. desired destination, duration of stay, budget, etc.). The agent would then autonomously select the best deal on both Lodgenta and other platforms, propose a full holiday experience, and, if authorised, book and arrange it on behalf of the user. This, however, requires Lodgenta to evaluate compliance considerations across various areas. For instance, while many obligations will sit upstream with the third-party model provider, Lodgenta's integration and deployment choices carry their own implications and duties.

### Lodgenta's online ecosystem




### Actions that Lodgenta should take

1. **Transparency and online safety:** Given the agent is interacting directly with users it may be in scope of incoming EU transparency rules. Lodgenta should make clear users are interacting with AI. Additionally, where applicable, Lodgenta should assess for illegal content risks and risks to minors and implement mitigations (e.g. providing clear reporting mechanisms for user-generated listings and age assurance to enforce minimum age requirements set out in T&Cs).
2. **Triggering additional regulatory obligations:** A highly autonomous agent risks drifting into high-risk EU AI Act use cases, for example assessing creditworthiness to offer finance options, or into other regulated activities, such as financial advice. Unless Lodgenta is prepared to meet the additional obligations these activities entail, it should constrain the agent's functionality with specific guardrails and avoid inadvertently expanding its regulatory perimeter, for example by preventing the agent from assessing a user's affordability or recommending specific financing products and routing any regulated queries to an authorised human adviser. Lodgenta should also implement safeguards to prevent deceptive or manipulative techniques that materially distort user behaviour and are likely to cause significant harm, which are prohibited under the EU AI Act.
3. **Choice outsourcing:** To ensure compliance with consumer law, Lodgenta should ensure users remain able to make informed, active decisions. For example, drawing on UK CMA work in this area, appropriate safeguards may include requesting explicit user confirmation before high-risk actions. The agent should consistently disclose key information (e.g. pricing and commercial context), with clear accountability, monitoring, and escalation where outcomes fall outside defined parameters.

© 2026 Deloitte LLP. All rights reserved.

# 7. Enhanced cross-border oversight

## Prepare for greater responsibility over imported goods, product requirements and fulfilment

Greater regulatory oversight of cross-border e-commerce means that marketplaces are taking on greater compliance responsibility for how goods enter and move through different jurisdictions. This requires strong seller and product governance and effective customs data capabilities.

### Regulatory areas

**Trade:** In the EU, under the new Union Customs Code (UCC), marketplaces may become "deemed importers", introducing new liabilities for import duties, VAT and product compliance. Importers will also need to submit customs data to a centralised hub, while the removal of the €150 duty exemption and planned handling fees may increase import complexity.

**Sustainability:** Sustainability requirements are increasingly relevant to goods placed on the EU market, including product information, traceability, packaging and lifecycle controls. For marketplaces, this may increase the need to collect and validate product-level information from sellers.

### Key Considerations

- **Assess where platform-level import liability may arise.** Marketplaces should identify where "deemed importer" status may apply and embed controls to manage responsibility for import duties, VAT and product compliance.
- **Build customs data capabilities ahead of the EU Customs Data Hub.** Marketplaces should improve data quality, governance and systems readiness for centralised customs reporting from July 2028.
- **Strengthen seller and product governance before goods enter the EU.** Accurate product classification, valuation, origin and seller information will become increasingly important, supported by proportionate checks on sellers and listings.
- **Prepare for the end of the low-value duty exemption.** The removal of the €150 exemption and the introduction of a flat €3 fee for such products may create new customs processes and affect the commercial viability of lower-value non-EU imports.
- **Assess the impact of handling fees on low-value imports.** Per-item handling fees may reduce the commercial viability of low-value imports and create operational challenges, compounded by differing implementation across Member States.
- **Evaluate emerging e-commerce warehouse models.** Goods held under customs control prior to sale may reduce handling fees and improve returns management, but may require operational changes, for example in relation to inventory management and tracking.
- **Apply financial crime controls to trade-specific sanctions risks** (see *page 16*). Sanctions controls should reflect geographic, product, customer and transaction risk, supported by screening, due diligence and monitoring.
- **Factor sustainability requirements into trade controls.** Product information, traceability and packaging requirements may affect seller governance, fulfilment and returns.

### Regulatory expectations arising from sustainability regulations

1. Sustainability obligations are increasingly spanning the end-to-end product lifecycle, from how goods are sourced and described to how they are produced, used and disposed.
2. The Ecodesign for Sustainable Products Regulation introduces mandatory product performance and information requirements, via a Digital Product Passport (DPP), for some products placed on the EU market. Whilst the DPP's scope is initially narrow, priority categories including textiles, mattresses and furniture will require a DPP from 2027, with electronic products from 2030 onwards. In addition, as part of the upcoming European Product Act, the Commission is considering whether the DPP may also be used to prove products' conformity, supporting the EU's circular economy objectives while addressing inadequate practices of notified conformity assessment bodies.
3. This comes alongside the EU Deforestation Regulation, Corporate Sustainability Due Diligence Directive and Packaging and Packaging Waste Regulation. As a result, sustainability is moving from a reporting exercise towards a practical condition for placing and moving goods through the EU market.
4. For marketplaces, this means embedding sustainability requirements into seller governance, product information controls and fulfilment processes, so goods can be listed, imported, fulfilled and returned in a compliant way.

© 2026 Deloitte LLP. All rights reserved.

# 8. Scale as a regulatory trigger

## Monitor growth against thresholds which, if crossed, result in enhanced risk assessment, reporting and audit requirements

As marketplaces grow, regulatory expectations can increase. Marketplaces should monitor growth against thresholds and ensure preparedness, for example through a readiness roadmap.

### Regulatory areas

**Online safety (EU):** Services reaching 45 million monthly active recipients in the EU may be designated as VLOPs under the DSA, triggering enhanced requirements including systemic risk assessments, audits and data access requirements.

**Online safety (UK):** Ofcom will designate 'categorised services' based on size and functionality, triggering additional obligations including transparency reporting and risk assessment disclosures.

### Key Considerations

- **Monitor growth against key regulatory thresholds.** Track user numbers, geographic reach and feature evolution to anticipate DSA VLOP designation or OSA categorisation.
- **Assess the regulatory impact of new features before launch.** Features such as recommender systems, messaging or resharing may trigger OSA categorisation or new obligations under the regime.
- **Develop a Day 1 readiness roadmap.** Identify governance, controls, ownership and resourcing necessary to comply. Under the DSA, newly designated VLOPs have just four months to comply with enhanced obligations.
- **Build scalable data and reporting capabilities early.** Larger services require reliable, repeatable data to support DSA systemic risk assessments, transparency reporting and audits.
- **Prepare for Ofcom's bespoke approach.** Categorised services or services approaching the thresholds should ensure readiness to engage with Ofcom transparency notices, including the feasibility of reporting requirements.
- **Monitor the evolving UK regime.** Beyond transparency obligations, Ofcom's categorised services regime is still developing, with further detail on incoming obligations expected.
- **Align UK and EU compliance approaches where possible.** Despite differences in approach, marketplaces should seek to align risk assessment, reporting and governance processes where feasible to avoid duplication.

### Regulatory expectations for designated services

#### EU DSA: VLOPs

- Establish an **independent compliance function**
- Conduct **systemic risk assessments**, including risks related to illegal content, protection of minors and broader societal harms
- Implement **mitigation measures** to address identified risks
- Undergo **independent audits** of risk assessments and controls
- Provide **enhanced transparency** on moderation, advertising and recommender systems
- Provide non-public **data access** to vetted researchers
- Establish **internal complaint-handling systems** and clear points of contact

#### UK OSA: Categorised Services

- **Submit risk assessments** to Ofcom and **publish summaries**
- **Publish transparency reports** based on bespoke transparency notices
- Prepare for **additional duties** as the categorised services regime develops

© 2026 Deloitte LLP. All rights reserved.

# Annex

- **The e-commerce ecosystem**: A taxonomy of the e-commerce and online marketplace ecosystem.
- **Mapping an online marketplace**: Illustrative view of the online marketplace value chain, mapping key activities and features.
- **Legal and regulatory glossary**: Laws and regulations relevant to the content of this report.
- **Authors and contacts**: Report authors and who to contact for a follow-up conversation.

© 2026 Deloitte LLP. All rights reserved.

# The e-commerce ecosystem

## A taxonomy

Throughout this report, we define e-commerce as the buying and selling of goods and services over the internet (e.g. via a website, smartphone app or social media platform). Here, we define the main categories* of e-commerce platforms, which include online marketplaces, the core focus of this report. We also highlight platforms that do not directly allow the sale of products and services but instead enable discovery and comparison.

### E-commerce platforms

Online platforms enabling businesses or consumers to sell their products and services. This could be a website, a marketplace, mobile app or social media storefront.

### E-commerce websites

Websites selling products and services directly to buyers.

**Own-brand web store**
Selling only own branded products and services.

**Retailers**
Inventory includes third-party and potentially own-brand products.

### Core focus: Online marketplaces

**Product-based**
Platforms enabling third-party sellers to list products for consumers to browse, compare and buy.

- **Hybrid**: Platform sells own inventory while also hosting third-party sellers.
- **Third-party only**: Platform hosts third-party sellers only and does not hold inventory or sell directly.

**Service-based**
Platforms connecting customers with providers of a particular service, such as food delivery, ride sharing, and home maintenance.

**Renting / sharing assets**
Platforms enabling rental or sharing of various assets, such as vacation homes or vehicles.

**Coupon platforms**
Platforms connecting consumers to goods, services and experiences by offering discounted vouchers.

### Discovery / comparison platforms

Platforms enabling the sharing of information to enable e-commerce. Transactions based on that information are concluded outside the platform. For example, travel search engines, comparison sites and booking apps.

### Emerging trends for online marketplaces

**Social commerce**
Social media platforms used to buy, sell and promote products and services.

**Livestreaming**
Livestream-based promotion of products that consumers can buy in real time.

**Agentic commerce**
Shopping powered by AI agents that act on behalf of consumers, from search to checkout.

**AR/VR technology applications**
Augmented Reality (AR) and Virtual Reality (VR) enable immersive shopping experiences, e.g., by allowing consumers to interact with a product in their real surroundings.

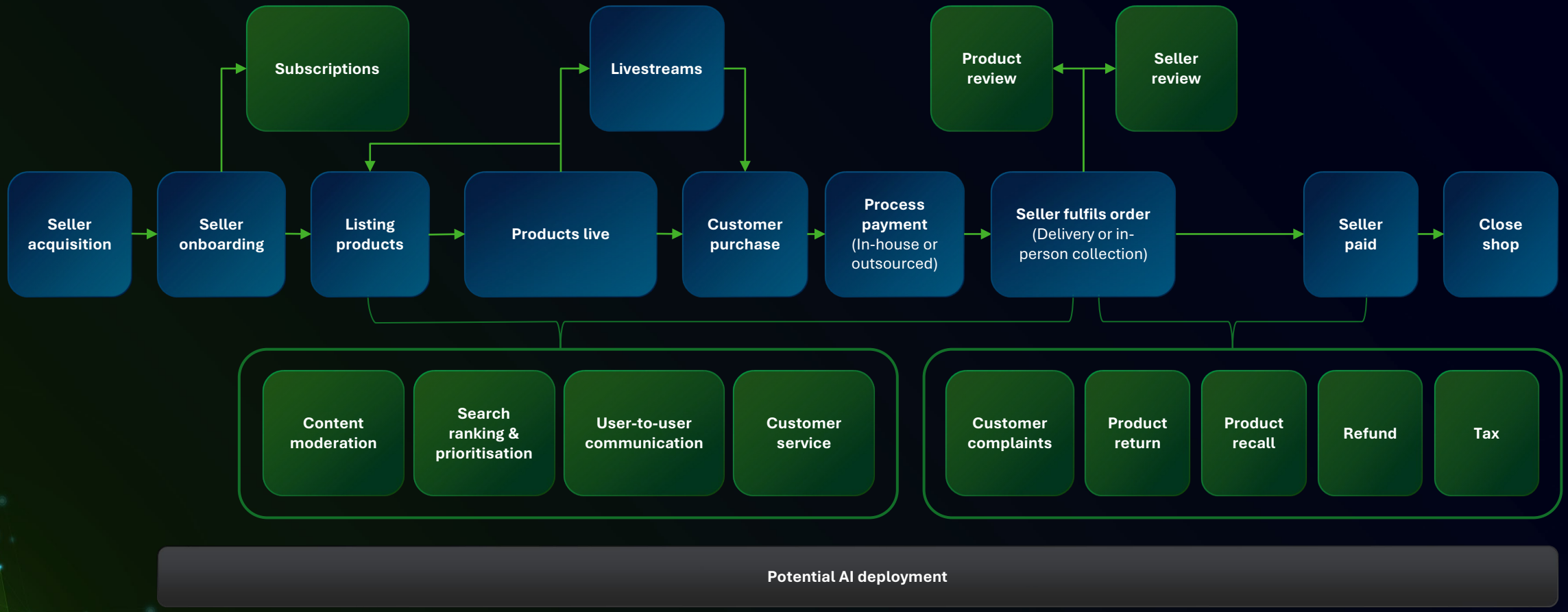
**Not mutually exclusive. Platforms or services may operate across multiple models depending on their functionalities.*

© 2026 Deloitte LLP. All rights reserved.

# Mapping an online marketplace

## Selected activities and features of a typical online marketplace

The below provides a high-level, illustrative view of the online marketplace value chain, mapping key activities and features. While this value chain is particularly relevant to product-based online marketplaces, many elements also apply to other marketplace or e-commerce models. Some elements represent core functions common to most marketplaces, such as product listings, payments and fulfilment, while others are optional or emerging, such as livestreaming or subscriptions, and may not be present across all marketplaces.




© 2026 Deloitte LLP. All rights reserved.

# Legal and regulatory glossary

## EU and UK laws and regulations relevant to this report

| | EU | UK |
|---|---|---|
| **Online Safety** | • Digital Services Act (DSA) | • Online Safety Act (OSA) |
| **Consumer Fairness** | • Unfair Commercial Practices Directive<br>• (planned) Digital Fairness Act (DFA) | • Digital Markets, Competition and Consumers Act (DMCCA) |
| **AI** | • Artificial Intelligence Act (AI Act) | • The UK has a principles-based regulatory framework for AI, which regulators implement in their sectors by applying existing laws and issuing supplementary regulatory guidance as required. |
| **Financial Crime** | • Anti-Money Laundering Directive (AMLD)<br>• Financial Sanctions Lists | • Proceeds of Crime Act, Money Laundering Regulations<br>• Sanctions and Anti-Money Laundering Act<br>• Economic Crime and Corporate Transparency Act |
| **Product Safety** | • General Product Safety Regulation (GPSR)<br>• (planned) European Product Act (EPA) | • Product Regulation and Metrology Act<br>• (planned) UK Product Safety Framework to replace the UK General Product Safety Regulations (GPSR) |
| **Trade** | • EU Customs Reform<br>• Trade Sanctions Lists | • Taxation (Cross-border Trade) Act<br>• Low Value Imports (LVI) customs reform (HM Treasury consultation, 2025–2026) |
| **Sustainability** | • Corporate Sustainability Due Diligence Directive (CSDDD)<br>• Ecodesign for Sustainable Products Regulation (ESPR)<br>• Packaging and Packaging Waste Regulation (PPWR) | • Extended Producer Responsibility (EPR) for packaging |

*These icons are used to map relevant regulatory domains across each of the eight priority areas in pages 6 to 16.*

© 2026 Deloitte LLP. All rights reserved.

# Authors and key contacts

## EMEA Centre for Regulatory Strategy

**Suchitra Nair**
Partner
snair@deloitte.co.uk

**Robert MacDougall**
Director
rmacdougall@deloitte.co.uk

**Nick Evans**
Senior Manager
nickaevans@deloitte.co.uk

**Matteo Orta**
Manager
morta@deloitte.co.uk

**Giulia De Bernardi**
Assistant Manager
giuliadebernardi@deloitte.co.uk


*This report was written by Deloitte's EMEA Centre for Regulatory Strategy (ECRS). The ECRS is a source of critical insight and advice, designed to assist clients to anticipate change and respond with confidence to the strategic and aggregate impact of regulation.*

## Digital Regulation

**Nick Seeber**
Partner
nseeber@deloitte.co.uk

**Laurie Gilchrist**
Director
lgilchrist@deloitte.co.uk

**Jessica Matthews**
Assistant Director
jjmatthews@deloitte.co.uk


## Financial Crime

**Amber Andrade**
Partner
amandrade@deloitte.co.uk

**Garikai Mparutsa**
Director
gmparutsa@deloitte.co.uk



## Acknowledgements

*The authors would also like to thank Abi Briggs, Valeria Gallo, Sam Kiely, Guy Stocks, Bradley Roberts, Ed Smith and Marios Leonidou for their contributions to this publication.*


© 2026 Deloitte LLP. All rights reserved.

Deloitte.

*Together makes progress*

This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 1 New Street Square, London EC4A 3HQ, United Kingdom.

Deloitte LLP's affiliate (Deloitte Management Services Limited) is a shareholder in Deloitte EMEA BV (Deloitte EMEA). Deloitte EMEA is a member firm of Deloitte Touche Tohmatsu Limited (DTTL). DTTL and Deloitte EMEA do not provide services to clients. Services may be provided by other Deloitte entities within the global network of member firms, each of which are separate and independent legal entities. Please see www.deloitte.com/about to learn more about our global network of member firms.

© 2026 Deloitte LLP. All rights reserved.

MAKING AN IMPACT THAT MATTERS since 1845