MatchGroup

2025

DSA Safe Dating Report

April 10, 2025

At Match Group, our mission is to spark meaningful connections for every single person worldwide.

The services we provide across our portfolio reflect our commitment to making online dating the safest way to meet people in the world, from the moment someone creates their profile to when they meet in real life.

While trust and safety is foundational to every platform's success, it is uniquely important to online dating services. Nearly 15 years ago, I started my career studying safety and privacy on the earliest generation of dating apps, and saw how important it is for companies to invest in these areas. Today, I have the privilege of leading Match Group's efforts to ensure our apps are safe, trustworthy, and inclusive for all — and have seen firsthand how this work is at the heart of our mission and our business.

Match Group and its brands are focused on identifying best-in-class approaches to protecting our users — and using what we learn to improve every brand in the Match Group portfolio, including Tinder®, Hinge®, Azar®, Meetic®, OkCupid®, Plenty of Fish®, and The League®. This work includes driving innovative solutions to combat spam and fraud, strengthening partnerships with industry experts, and implementing new proactive policies and measures to protect our users — all while staying ahead of emerging safety challenges in the online dating space.

Across the EU, Match Group has approximately 17 million monthly average users across seven platforms, all of which are aimed at creating safe, authentic, inclusive spaces for people to find connection, no matter who you are or where you're from. This diversity of apps is a key part of our trust and safety strategy. We develop innovative approaches available to all users across our portfolio of brands, and then take steps to implement best practices that have the opportunity to enhance safety company-wide.

Almost 30 years ago, Match.com introduced online dating to the world. Today, we're continuing to innovate across platforms like Tinder, Hinge, and Meetic — all in service of our mission to help people spark and form meaningful connections. As we continue to evolve, I am confident that Match Group's efforts — guided by a focus on safety by design, user control, authenticity, and inclusivity — will continue to lead the industry in delivering the safe experiences our users expect.

We are proud to publish our first-ever transparency report today outlining how we keep our users safe. We look forward to working with the European Commission and governments and law enforcement in the European Union in our compliance with the Digital Services Act (DSA).

––––––

Yoel Roth
Head of Trust & Safety, Match Group

Introduction

Match Group[1] is on a mission to spark meaningful connections for all users around the world. As leaders in the online dating category, we innovate and champion industry best practices that are designed to help make online dating safe and inclusive for everyone. Match Group offers a portfolio of brands that operate a diverse array of leading online dating and social connection platforms that collectively have millions of users who are seeking various types of human connections. Our largest brands in the European Union (EU) include Tinder and Hinge, as well as our localized Meetic brands.

Context for this report

In this report, we are reporting data about content moderation, appeals, legal process orders, and other aspects of our trust and safety efforts in the European Union for the period of 17 February 2024 to 16 February 2025. More than 99.88% of average monthly users across our platforms in the EU use our apps without a serious violation of our policies, on- or off-platform. We believe that any report of harm is one too many, and we remain deeply committed to ensuring the safety and well-being of our users.

During the past year, Match Group's trust and safety, legal, and engineering teams have worked together to prepare this report. As part of this process, we harmonized our policies across our many diverse brands, as well as with the DSA defined categories. In some instances, certain DSA categories did not perfectly align with the content and behavior found on online dating and social connection platforms. For example, categories that focus on negative effects of civic discourse or elections, self-harm, consumer information infringements, and unsafe or prohibited products are not typically relevant to online dating platforms, which lack viral or public content and marketplace functions like social media platforms. Therefore, we have made a best effort to reconcile these categories with our platforms.

The portfolio nature of our business

While Match Group's commitment to safety and respect is shared across all our brands, the portfolio nature of our business is an important consideration for this report. It enables us to continuously learn from our various brands and share relevant information and best practices to improve our overall trust and safety policies on an ongoing basis. As an example, when we ban an account in response to a report of a severe on- or off-platform issue on one brand, we proactively remove that account across all brands in our portfolio.

Our brands are each exploring unique approaches and features, which require tailored safety products and policies to meet their specific needs. Users of Match Group's brands also seek different types of connections, which come with different user expectations for their interactions on our apps, and our online dating platforms are built differently to meet these different needs. These distinctions can be seen at both the product and policy level.

Addressing off-platform conduct

Match Group's platforms are different from most of the other platforms subject to the DSA because our apps are focused on bringing people together online and, ultimately, face to face. Consequently, our approach to content moderation is designed to help protect users both online and in real-life interactions. In this report, we include data on illegal content, reviews, and actions we take to keep our apps safe and authentic, including actions we take as a result of user reports about conduct that occurs off our platforms. For example, if someone tells us that they received harassing messages from another person on a messaging platform outside of our apps, we would consider those off-platform actions as part of our efforts to help keep our users safe. Where programmatically available to us, we also employ data from governments and law enforcement about sex offenders and individuals with violent criminal histories to keep potentially harmful individuals off of our services.

We recognize that some connections made using online dating platforms can potentially lead to harm in the real world. Gender-based violence and any form of sexual or physical violence are abhorrent and not tolerated on or off our platforms. We believe that even one instance is too many, and it's our goal not only to prevent these instances on our platforms, but also to increase awareness of what needs to be done to combat this issue at a societal level.

If a user reports that they've experienced some form of harm when they met outside of our apps, we take immediate steps to support the reporter and enable law enforcement investigations. Unlike reports about online behavior or content, we can rarely verify reports of off-platform misconduct because we do not have the information to do so. We take these reports seriously and take action on the account in question even when we cannot confirm the accuracy of the report with 100% certainty. We also provide users who have submitted reports with access to crisis resources and survivor support.

Our approach to responding to law enforcement centers on providing verified, actionable data in a timely fashion. Through Kodex, our dedicated law enforcement portal, we prioritize sharing information that reflects our industry-leading safety practices and meaningful user protections. As part of our transparency efforts, we disclose reports referred to law enforcement as a way to provide clear and reliable data that users and other stakeholders can trust. We continuously evaluate and enhance our safety initiatives to ensure that we're not only meeting but exceeding the highest standards in protecting our users.

Fewer than 0.1% of our users have reported off-platform misconduct during the period covered in this report. Due to the serious nature of these reports and our victim-centric approach, this is an area where we are actively investing, coordinating across our platforms, and working with others to improve how we handle such reports.

Our Commitment to Safety

Match Group's online dating platforms bring together people looking for meaningful connections. Through the enforcement of our policies, we strive to uphold high standards of safety, authenticity, and respect for everyone.

Guiding principles

Our overarching commitment to safety gives people the tools and confidence they need to safely and authentically form real and respectful connections. Four pillars guide our approach and policies:

Safety by Design

We believe trust and safety is about developing services that are resilient by design to misuse, and which help mitigate safety issues before they happen. This means identifying risks early in the design phase — ensuring that all new features are built with user safety at the forefront. Regular assessments and reviews further ensure that we are continuously addressing safety risks across all services.

User Control

We help ensure that our users can have the interactions they want, when they want them, and have clear and easy ways of dealing with unwanted content and conduct.

Authenticity and Trust

We foster genuine connections between real people. We give users effective tools to demonstrate that the people they meet are who they say they are.

Inclusivity

We build platforms for people of all identities, backgrounds, and orientations. We work to ensure our platforms are a welcoming place for our global users.

Safety policies

In line with the guiding principles that support our commitment to safety, we enforce a variety of specific policies:

- **Keeping bad actors off our platforms.** We invest heavily in technology and operations to proactively protect our apps. This includes our efforts to keep people with potentially dangerous offline conduct off our services. Where available, we employ data provided by governments and law enforcement to keep registered sex offenders and anyone suspected of sex trafficking from using our platforms.

- **Enforcing child safety protections.** Child safety is an ecosystem-wide priority for all platforms. We work diligently to play our part in keeping ineligible users, including underage users, off our platforms using a combination of technology and human review. We've built comprehensive tools to ensure our platforms prevent the distribution of and support proper reporting of any child sexual abuse material (CSAM).

- **Addressing hate speech.** Hate speech has no place on our platforms. In addition to using a combination of automated and human review to identify prohibited speech, we encourage users to report prohibited content they encounter using our in-app features so that we can take action.

- **Prohibiting prostitution, sex trafficking, and solicitation.** Promoting or advocating for commercial sexual services, human trafficking, or other non-consensual sexual acts is strictly prohibited and results in being banned from all Match Group platforms. Solicitation of any kind is also prohibited.

- **Banning and blocking fraud and scams.** Match Group has a dedicated team and sophisticated technology that bans and blocks spam, scams, and fraud using a variety of tools including conducting automated or manual reviews of each user profile to block certain IP addresses from high-alert countries, identify stolen credit card numbers, and detect suspicious language in profiles. For example, on Tinder, users may be proactively informed if they have matched and interacted with another user whose account is then flagged for potentially fraudulent behavior. Match Group's brands educate users to never send money to someone they met on our platforms, and to report any individual who asks that they do. These steps are designed to stop scams in their tracks and help protect the next potential victim.

Safety features

We work to prevent and disrupt conduct that violates our policies by utilizing technology including AI, machine learning, natural language processing, and behavioral heuristics. When we create new features, we design for safety and authenticity from day one. Our teams conduct detailed assessments of potential risks, extensively test new features before they launch, examine possible outcomes in a controlled environment, and work with technology teams to implement the right safeguards. We are committed to using available data gathered from our brands to make improvements on an ongoing basis. This approach allows us to continuously learn and iterate in real time.

Match Group developed Share My Date, an in real life safety feature that our brands are incorporating and customizing. Share My Date allows users to share details of an upcoming date through a web link with friends and family to make dating safer and more fun.

Our Commitment to Safety

At Tinder, we developed Traveler Alert, an in-app safety notification that alerts users when they are located in areas where identifying as LGBTQIA+ is criminalized. This alert protects users in places where their safety might be at risk. Once the alert is activated, users can make a more informed choice about whether to have their profile remain hidden while in that location or opt in to making their profile public so that they can connect with new people.

Traveler Alert

Selfie Verification

Here are examples of our safety features, pioneered by Tinder and our other apps
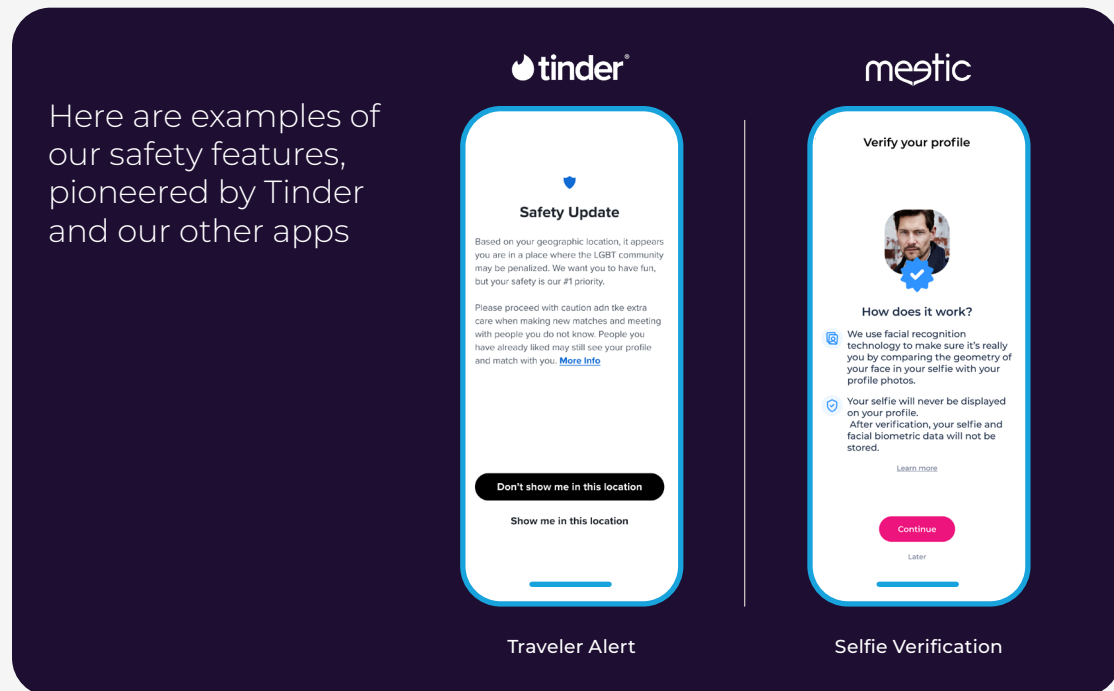
Another important part of our commitment to safety is educating our users. Each of our brands offers safety information and tips to empower users to make smart and safe choices while interacting on our platforms.
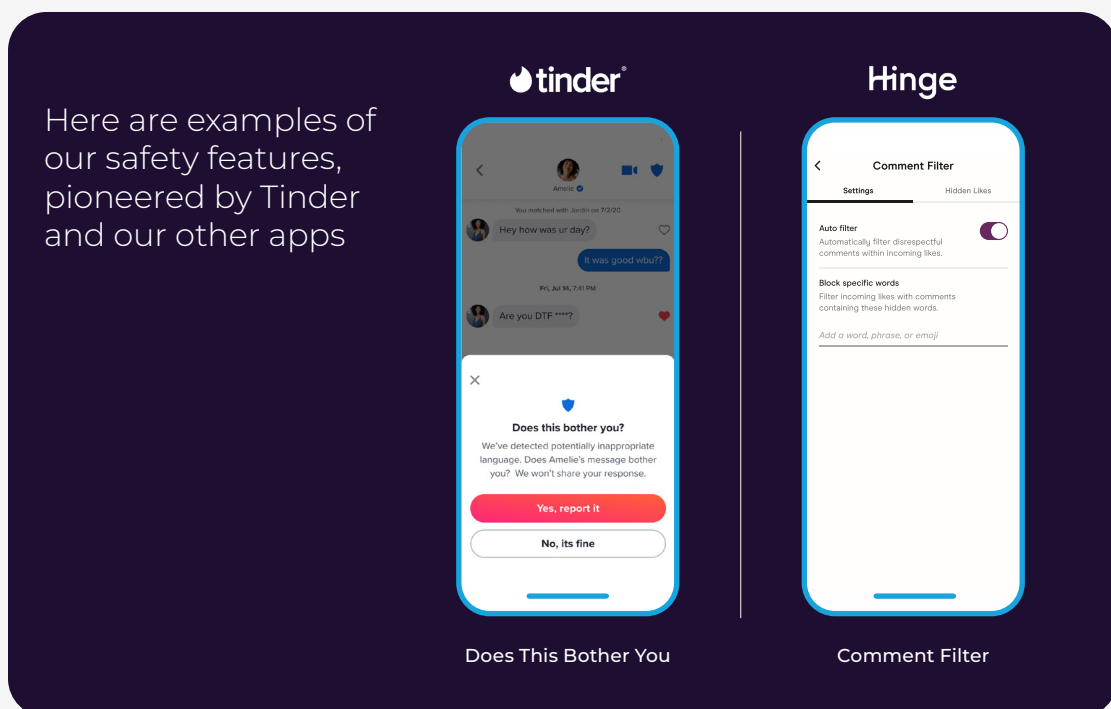
As an example, we have deployed our Are You Sure (AYS) prompts on Hinge and several of our Emerging & Evergreen brands, after originally introducing the feature on Tinder in 2021. AYS is a real-time warning system designed to help users engage in mutually respectful conversations. It uses AI to detect harmful language and proactively intervenes to warn the sender their message may be potentially harmful, asking them to pause and reconsider before sending it. The AI was built based on past user reports, and it will continue to evolve and improve over time. We prompt users 67 times per minute on Tinder to reconsider sending a message that our systems detect as potentially abusive or harmful. One in five users who receive an Are You Sure prompt on Tinder and Hinge change their behavior and edit or delete a potentially abusive or harmful message before it is sent.

Proactively checking in with users about potential safety issues is a critical part of our trust and safety toolkit. For example, Does This Bother You is an in-app prompt designed to enhance user safety and improve reporting on Tinder. This feature appears when users are exposed to potentially uncomfortable or harmful content. By asking users directly whether the content bothers them, we are able to gauge their comfort level and if the user indicates that the content does bother them, they are seamlessly directed into our reporting flow for review by our moderation team. In 2024, we showed users more than 174,000,000 Does This Bother You prompts to encourage reporting. The streamlined integration of this prompt helps lower the barriers to reporting — making it easier for users to take action when they encounter problematic content, increasing the likelihood of early intervention, and enabling a more user-friendly experience in addressing potentially harmful behavior. We plan to expand this feature to Hinge this Spring.

Hinge's Comment Filter provides users with the ability to proactively filter language they don't want to see, helping to deter negative interactions before they start. Users have the ability to send a comment when they like something in a profile, which is often a first point of contact. If the content of a Like with Comment includes a word, phrase, or emoji that the receiving user has added to their personalized filter list, it is moved to a separate message category where users can choose to review it or delete without opening. In its newest iteration, Comment Filter also offers an AI-powered auto filter option for users who prefer not to create a custom list, but still want to avoid language that could potentially be offensive. Users can use either function or both simultaneously.

On Hinge, we also follow up with users after they connect via the We Met in-app survey. This feature asks each person privately if they went on a date and if their match was the type of person they'd like to see again. If a user indicates that they do not want to meet their match again, they are given the option to make a report.

Here are examples of our safety features, pioneered by Tinder and our other apps

Does This Bother You

Comment Filter

Working with partners

Partnering with safety experts, NGOs, and law enforcement around the world allows us to stay on top of the latest trends, helps inform our continued investments in technology, and guides our ongoing policy enhancements. Our worldwide partnerships are an important part of the work we do — not only supporting our approach to content moderation but also making sure we reach our users offline.

In the EU, we partner with a wide range of organizations, such as the Fondation des Femmes (Women Foundation), Consentis (Consent), Fédération Nationale Solidarité Femmes (National Women's Solidarity Federation), HandsAway, and Hally in France; Lambda and LFSH in Germany; Centrum Seksueel Geweld (Center for Sexual Violence) in the Netherlands; and Fundación ASPACIA (ASPACIA Foundation), Amnistía Internacional (Amnesty International), Somos Estupendas, ANCEME, and Cruz Roja (Red Cross) in Spain.

We conduct regular safety campaigns with our partners on the ground in the EU. For example, in 2023 and 2024, we launched Healthy Dating Guides in partnership with NO MORE across eight European countries — Germany, Spain, Sweden, Norway, Denmark, Italy, France, and the Netherlands — in their native languages on Tinder, Hinge, and Meetic. The guides provide actionable steps and considerations for every stage of the dating journey. Users clicked on the guides more than two million times across Tinder, Hinge, Meetic, and OurTime (part of the Meetic family of brands) in the first days of the campaign and there have been nearly 400,000 views of the guides on NO MORE's website to date.

Tinder also launched an in-app campaign promoting information about how to access sexual assault resources and support in partnership with Centrum Seksueel Gewald in the Netherlands. Tinder partnered with Somos Estupendas on a campaign promoting tips for healthy and safe dating in Spain in order to create authentic connections and prioritize mental health and well-being.

Beginning in 2023 and throughout 2024, we conducted in-person safety roundtables in the UK, Spain, the Netherlands, and Germany, bringing together more than 20 organizations committed to fighting sexual abuse and online violence.

We also work with regional safety experts to inform our education work locally. For example, in France, Match Group partnered with Fédération Nationale Solidarité Femmes to provide a resource document, released to the public alongside the guides, on how to recognize violence and respond to victims.

In 2023, Match Group also launched our first global romance scam campaign across our portfolio, in partnership with the International Association of Financial Crimes Investigators and victim advocates, to regularly educate users on how to spot, prevent, and report romance scams across Tinder, Hinge, Match, OkCupid, Plenty of Fish, OurTime, and Meetic. Since launch, users in more than 15 countries have seen these warnings and tips on how to protect themselves against online scams.

In 2025, we've supported the founding of ROOST, a nonprofit global community effort led by Google, OpenAI, and Discord among other leading companies and institutions, to build scalable and resilient safety infrastructure for the AI era. ROOST's tools focus on child safety, foundation model-powered content safeguards, and core safety infrastructure.

We don't do this alone. Match Group partners with leading safety experts, nonprofits, and advocates to improve protection for our users. From policy advisors to technology innovators, our network of experts helps us lead the industry in trust and safety.

Our Approach to Content Moderation

Match Group is proud to be an industry leader in online safety, and we make significant investments in our trust and safety work. Match Group and each of its brands have teams dedicated to trust and safety, with content moderators and other colleagues across the EU. We also partner with external service providers to carry out content moderation.

Human moderation, assisted by machine learning and automation

Human moderators review content and accounts that have been flagged by automated systems or by user reports, and act on those reports according to our policies and guidelines. We train moderators on our global standards while integrating local cultural insights, ensuring consistent enforcement of our terms of service worldwide. We regularly hold education sessions on new or developing trends and topics. We also regularly hold learning sessions across Match Group to help educate and provide resources on safety and accessibility topics such as intersectionality and cultural literacy, sexual assault and harassment, inclusivity for marginalized groups, romance scams, and domestic violence prevention.

Our human and automated moderation efforts are closely linked. Like many other platforms, we augment the efforts of our human content moderators with digital tools — building on technological capabilities to analyze large amounts of data at speed and scale, while directing human efforts toward nuanced reports.

Our detection features flag messages with spam or potentially inappropriate language in real time and, in some cases, encourage the user to edit the message before it's sent. A majority of our spam enforcements are automated, and most are based on ML/AI or behavioral heuristics. These features help improve user behavior and educate users on how to appropriately interact with others. We also use the data and insights gained through the use of these tools to make moderation improvements in real time and apply lessons learned across our portfolio of brands, where relevant.

Support for content moderators

We are aware that content moderation can expose moderators to potentially difficult experiences, which is why we invest in and prioritize their well-being, offering them a range of wellness and resiliency programs. The following initiatives are examples of our commitment to supporting the mental and emotional well-being of both our in-house teams and contract moderators:

- Our Tinder and Hinge teams have partnered with Zevo Health, a counseling service for content moderators that provides group sessions and one-to-one support.

- Hinge holds regular "Deep Dives" for complex user cases so that decisions do not rest solely on individual moderators, promoting collaboration and reducing emotional burden.

- Our Business Process Outsourcing partners that support Match Group's internal teams have onsite therapists available for use at any time, providing immediate access to mental health resources.

Central and brand-specific policy

We aim to align our policy and enforcement efforts across Match Group — but, in certain instances, there may be minor content moderation policy differences between our brands. For example, certain content on one platform may be permitted, whereas it may result in a ban on another. These differences reflect our efforts to balance detecting and proactively removing bad actors, hate speech, fraud, and other types of content while also ensuring that each brand can address the specific risks and behaviors of its unique user base. For the purposes of this report, every brand has made a best effort to map its own policies to the DSA categories. Moving forward, we will further standardize our policies where it makes sense, while continuing to ensure that each brand can tailor its approach as needed.

Conclusion

The work described in this report is ongoing — we are continuously investing in and enhancing the safety of our platforms for our global users. In line with this commitment, we are planning to advance the following actions and initiatives in the coming months, some of which are already in progress at the time of writing.

Global expansion of the Match Group Advisory Council

We are expanding our Match Group Advisory Council (MGAC) to include more global safety experts and advocates located in the EU and around the world. First established in 2018, the MGAC comprises leaders in the study and prevention of sexual assault, sex trafficking, abuse, harassment, and similar issues.

Policy taxonomy revision

To ensure consistency and parity in moderation and enforcement across the entire Match Group portfolio, we have undertaken a complete revision of our policy taxonomy. This revision harmonizes the categorization of violations across all brands, helping to streamline enforcement actions and improve transparency in how policy violations are addressed. This update also aligns our policies with evolving regulatory standards and user expectations, ensuring fair and effective moderation across all brands.

Proportionate enforcement for reports of off-platform misconduct

Our proportionate enforcement model is designed to ensure that every report we receive is addressed appropriately. By scaling enforcement actions based on the severity of the reported behavior, we maintain robust safety protocols for the most serious cases while also avoiding excessive banning for minor or unverified incidents.

Analysis on the use of generative AI by malicious actors

In 2024, we commissioned an independent analysis by AI deepfake detection platform Reality Defender of the prevalence of AI-generated images across Match Group apps. This analysis found that AI-generated images are rare on Match Group's apps, with 99.4% of Tinder and Hinge profile images showing no indication of AI manipulation. Even among the small percentage of manipulated images, further analysis found that most were due to the use of face-tuning or filters by real people, rather than malicious deepfakes. While AI-generated photos remain uncommon, Match Group is proactively addressing potential future risks by leveraging this research to develop educational materials in 2025, helping users recognize AI-generated content alongside existing scam prevention resources. We are also working to enhance detection and blocking capabilities for malicious AI content, reinforcing our commitment to authenticity and user safety in online dating.

Partnership with ThroughLine to provide accessible and globally inclusive crisis support

Match Group partners with ThroughLine, the world's largest verified network of crisis hotlines and helplines, to provide users with access to localized, high-quality support when they need it most. ThroughLine's database spans over 130 countries and covers 23 issue areas, including gender-based violence, scams, suicide prevention, and mental health support. Users can connect through multiple channels beyond traditional phone hotlines, such as SMS, online chat, and WhatsApp, ensuring accessible and immediate assistance in multiple languages. Integrating this resource across our portfolio reinforces our commitment to user safety and well-being, making support more comprehensive and globally inclusive.

Taken together, these initiatives reflect our commitment to continuous improvement and innovation in keeping our platforms safe, while ensuring that enforcement remains fair and consistent across the Match Group portfolio of brands. Publishing this report and regularly sharing data on our efforts are important parts of this process.

Appendices

Appendix I — Our Safety Data in Detail

The data below reflect aggregate numbers across Match Group's brands in the EU for the period of 17 February 2024 to 16 February 2025.

Appendix I.A — Own-initiative content moderation

We work to keep our platforms safe by proactively identifying violations of our policies, and then removing content and banning accounts.

Content removal

This table provides a breakdown of content removal broken down by the relevant policy. It also shows the number of items that were removed using automated moderation.

Own-initiative content removal (17 February 2024 – 16 February 2025)

TYPE OF POLICY	TOTAL CONTENT REMOVED	CONTENT REMOVED BY AUTOMATION (%)
Abuse and Harassment	638	6%
Allegations of Off-Platform Misconduct	20	0%
Illegal and Regulated Activities	5,209	2%
Non-T&S TOS Violations	3,992,780	38%
Other	434,258	17%
Sensitive Content	478,667	4%
Spam, Inauthentic, and Ineligible Accounts	372,000	11%
Violence and Hate	264	0%
TOTAL	**5,283,836**	**31%**

Account bans

Data on banned accounts is complex — the numbers alone do not tell the whole story. We ban an account when we believe that the user has violated our policies, which are designed to prevent harm and create a safe, authentic space for our users to connect.

There are several important contextual points to consider when comparing the number of user reports, violations, and banned accounts. First, a single user may be tagged to multiple reports and violations, resulting in fewer total bans than total reports and violations. Second, if a user's

accounts are removed from multiple platforms, it will result in multiple bans, but represents only one individual (and potentially only one report). Finally, a portion of banned accounts are users attempting to create new accounts after their previous accounts were banned.

A very significant portion of our content moderation actions — nearly 80% of the total account bans and suspensions during the reporting period — represent our efforts to identify and remove ineligible accounts from our services. Many of these actions are carried out proactively, including by screening for potentially inauthentic or underage users during or shortly after account creation. In addition to moderation at the account creation stage, we check profiles over time and investigate user reports of ineligible users.

As an alternative to bans, in some cases and for some brands such as Azar, we also use suspensions, i.e., time-limited access restrictions. We use suspensions for less serious violations of our rules that do not warrant a permanent ban.

This table provides the number of account bans and suspensions for violations of our policies, including the number of accounts actioned using our automated moderation technology.

Own-initiative account bans and suspensions (17 February 2024 – 16 February 2025)

TYPE OF POLICY	TOTAL ACCOUNTS BANNED OR SUSPENDED	ACCOUNTS BANNED OR SUSPENDED DETECTED PROACTIVELY (%)	PERCENTAGE OF ACTIVE USERS OVER THE REPORTING PERIOD[2]
Abuse and Harassment	46,783	36%	0.022%
Allegations of Off-Platform Misconduct	30,342	11%	0.014%
Illegal and Regulated Activities	26,301	36%	0.012%
Non-T&S TOS Violations	136,374	16%	0.065%
Other	49,293	100%	0.023%
Sensitive Content	1,886,310	27%	0.896%
Spam, Inauthentic, and Ineligible Accounts	9,225,333	58%	4.382%
Violence and Hate	6,896	41%	0.003%
Total	11,407,632	52%	5.419%

2   This figure is computed by dividing the monthly average of enforcements in the policy category during the reporting period by the average total monthly active users of our services in the EU.

Account bans / suspensions (17 February 2024 – 16 February 2025)

Total banned / suspended	11,407,632
Accounts banned / suspended detected proactively	5,931,728 (52%)
Accounts banned / suspended automatically	8,226,830 (72%)

Appendix I.B — User reports

Like most online platforms, we receive more reports than actual violations of our policies. We offer users effective and easy-to-use reporting functions, so they can alert us to concerning content and behavior, in addition to our own proactive content moderation efforts. We encourage our users to be vocal and active by providing them with at least two separate reporting mechanisms: in-app and a web-based form. Additionally, some Match Group brands also offer email or live chat services. Each brand provides FAQs in their help centers about how to report.

Across all parts of our business, we take a victim-centric approach and treat seriously what our users report to us, reviewing all valid reports of concerning behavior and taking appropriate action.

Match Group works with a number of leading NGOs to ensure that our reporting flows are effective and informed by lived experiences. We have an ongoing partnership with Hally in France to enhance our processes around sexual misconduct reporting, moderation, and response, and Hally specifically advised on our in-app reporting flows. We incorporated Hally's feedback into our flows, allowing our brands to prioritize serious reports and act quickly against bad actors.

In addition to these reporting options, we offer users tools like blocking and unmatching, regardless of whether the content is ultimately found to violate our policies. It is important to note that neither blocking nor unmatching (nor being blocked or unmatched) prevents a user from reporting. We also enable non-users to make a report without creating an account, and we allow users, non-users, and entities to flag content that they allege is illegal.

Due to some limitations in our current tooling, we do not always have complete attribution of an enforcement action to the report from which it originated. For example, in cases where a single account is reported multiple times or by different users, we would attribute our enforcement action to all the submitted reports, even though only one action may have been taken. In some cases, a user will file a report for one reason, but the account or content may end up being actioned for another reason because, upon review, the user's report does not accurately match the policy violation. We are actively exploring ways to improve the quality of our report and enforcement data in future reports.

We received a total of 9,785,611 reports, which corresponds to 13,162,153 unique items of content. 3,057,926 users were responsible for these reports. On average, 2.09% of our monthly active users reported violations of our terms and conditions. Based on these user reports, we took action against 4 items of content for violating local laws and 2,628,082 items of content for violating our policies. Because one user may be responsible for multiple reports and violations, the number of account bans is lower than the number of reports and violations. Also, one user may have accounts across several brands, and our data counts each ban individually, meaning that multiple bans may relate to only one individual.

The median time to action a report under our policies is 1 hour, and the median time to action a report based on local laws is 189 hours.

Number of user reports received (17 February 2024 – 16 February 2025)

CATEGORY OF REPORT	NUMBER OF USER REPORTS RECEIVED
Abuse and Harassment	955,046
Allegations of Off-Platform Misconduct	241,089
Illegal and Regulated Activities	48,317
Non-T&S TOS Violations	620,406
Other	232,340
Sensitive Content	3,621,858
Spam, Inauthentic, and Ineligible Accounts	3,898,786
Violence and Hate	167,769
TOTAL	**9,785,611**

Appendix I.C — Orders from government authorities

Match Group is proud to assist law enforcement in their investigations and help ensure that bad actors are brought to justice, and we work closely with regulators and other government agencies on an ongoing basis in compliance with applicable local laws. We use Kodex — a best-in-class technology platform for communicating with law enforcement — to make this coordination as seamless and swift as possible.

We respond to every valid request and inquiry we receive from law enforcement. However, we are not always able to provide relevant information in response to a request. There are many reasons why this may be the case, such as:

- No account exists or was created using the details provided

- We were unable to locate an account with the information provided in the request (e.g., law enforcement only provided a first name, screenshot, or details that did not yield an account)

- There were no records to produce (e.g., because the relevant account was deleted or did not have the type of content requested)

- Any records found were outside the requested time frame

- Law enforcement did not issue the request correctly

- The records were preserved in accordance with a preservation request but no request for production was ultimately made

Orders to provide information

The following table shows the number of orders Match Group received from EU member states to provide information. Using the Kodex system, we acknowledge receipt of such orders immediately by sending an automatic acknowledgment. The median time to handle such orders across all our brands is 8 hours. Where a country is not listed, we have not been contacted by a law enforcement agency in that jurisdiction.

Orders from government authorities in the European Union to provide information (17 February 2024 – 16 February 2025)

MEMBER STATE	ABUSE AND HARASSMENT	ALLEGATION OF OFF-PLATFORM MISCONDUCT	ILLEGAL AND REGULATED ACTIVITIES	NON-T&S TOS VIOLATIONS	SPAM, INAUTHENTIC, & INELIGIBLE ACCOUNTS	VIOLENCE AND HATE
Austria	0	1	1	0	6	0
Belgium	0	1	1	0	1	0
Bulgaria	0	0	0	0	1	0
Croatia	0	0	0	0	1	0
Cyprus	0	0	0	0	1	0
Denmark	0	0	0	0	2	0
Estonia	0	0	0	0	2	0
Finland	0	2	1	0	12	0
France	1	72	6	13	39	2
Germany	2	58	7	0	91	1
Greece	0	0	0	0	2	0
Hungary	0	1	1	0	1	0
Ireland	4	2	0	0	2	0
Italy	0	0	1	1	8	0
Lithuania	0	1	0	0	1	0
Malta	0	1	0	0	0	0
Netherlands	0	1	0	0	1	0
Poland	3	6	2	0	15	0
Portugal	0	3	0	0	3	0
Romania	0	0	0	0	4	0
Spain	4	10	5	4	18	0
Sweden	0	3	0	0	3	0
TOTAL	**14**	**162**	**25**	**18**	**214**	**3**

Category of illegal content

Orders to remove content

During this reporting period, we have not received any orders from law enforcement to remove content.

Appendix I.D — Complaints and disputes

Every user who has had content removed from our platforms or who has been banned from one of our brands due to a policy violation has the opportunity to appeal. Appeals are reviewed by a dedicated team of human reviewers who are separate from the content moderation team. This organizational structure ensures we assess every situation objectively and enables members of our team to correct and refine automated content moderation, as needed.

Match Group received 180,757 appeals from users who challenged a decision to remove their content or ban their account(s). We reinstated 54,431 accounts following an appeal. The median time to make a determination on an appeal is 2 hours and 51 minutes.

We inform our users that if they do not agree with an enforcement decision and the resolution of their appeal, they have the right to challenge the decision either in a relevant court or refer the decision to a certified dispute settlement body. During this reporting period, no users had submitted a report to a court or certified dispute settlement body.

Appendix II — Policy Definitions

The moderation categories referenced above reflect a Match Group-wide policy taxonomy that aligns community guidelines and standards across each of our brands. Definitions of each policy category are set out below.

POLICY CATEGORY	EXAMPLE SUBCATEGORIES	DEFINITION
Abuse and Harassment	• Non-Consensual Sharing of Private Information • Harassment • Abusive Behavior	Abuse and Harassment includes on-platform behavior, actions, or content that may cause emotional or psychological harm through the use of intimidation, humiliation, or non-consensual acts. This includes persistent and unwanted interactions that threaten someone's safety or well-being.
Allegations of Off-Platform Misconduct	• Allegations of Abuse and Harassment • Allegations of Physical Harm • Allegations of Sexual Exploitation • Allegations of Financial Harm	Allegations of Off-Platform Misconduct include reports alleging harmful behaviors or actions that occurred outside the platform that indicate a potential risk to the safety, well-being, or integrity of the user.
Illegal and Regulated Activities	• Child Sexual Exploitation and Enticement • Commercial Sex and Solicitation • Copyright and Trademark Infringement • Illegal Use and Regulated Goods	Illegal and Regulated Activities includes behaviors, actions, or content that violate laws or regulations or are subject to specific heightened legal controls on distribution, sale, or promotion. We also strictly prohibit any content, behavior, or actions that involve the sexual abuse or exploitation of minors, including attempts to groom or entice minors into sexual activities (on- or offline).

POLICY CATEGORY	EXAMPLE SUBCATEGORIES	DEFINITION
Non-T&S TOS Violations	• Ineligible Image or Profile Content	In certain cases, specific Match Group platforms may restrict particular behaviors under their terms of service, even if such behaviors do not represent a safety or authenticity risk.
Other		In limited cases, despite our best efforts, we may not have specific policy attribution for some moderation actions taken.
Sensitive Content	• Adult Nudity, Pornography, and Sexualized Content • Graphic Content • Controlled Substance Use • Suicide, Suicidal Ideation, and Self-Harm	Sensitive Content includes content related to adult nudity, pornography, sexualized content, violence and gore, substance use, and behaviors associated with suicide, suicidal ideation, self-harm, and disordered eating.
Spam, Inauthentic, and Ineligible Accounts	• Attempted Financial Exploitation • Ban Evasion • False Reporting • Impersonation • Spam and Inauthentic Accounts • Suspected Underage Users • Convicted Violent Offenders	Spam, Inauthentic, and Ineligible Accounts includes profiles that engage in inauthentic activities, evade bans, impersonate others, or are otherwise ineligible for account creation due to age or legal status.
Violence and Hate	• Hateful and Discriminatory Behavior • Threats and Wishes of Harm • Terrorism, Violence, Extremism, and Hate Groups	Violence and Hate includes on-platform content or behavior that incites, promotes, or glorifies bodily harm or hatred against individuals or groups. Violence refers to any form of physical harm, including threats, intimidation, and coercion, regardless of motivation or perceived intent. Hate involves behavior or content that demeans, marginalizes, or incites violence against individuals or groups based on an actual or perceived association with a protected characteristic or class.

Appendix III — Reporting Functions Across Brands

When users encounter content or behavior they believe violates our community guidelines or terms of service, we provide them with easy-to-use reporting options to flag the behavior to us for review. These reporting functions are implemented slightly differently by each of our brands. Additional details about the reporting mechanism used by several of our largest Match Group brands are set out below.

tinder

Permits users to report other users, whether the other users are simply shown in their recommendation stack or they are users they have matched with. Users can access in-app reporting options in various ways, including through their profile screen, message inbox, and match list. Depending on which screen the reporting mechanism is accessed through, a different set of reporting options are available to the user, but generally include underage users, nudity or sexual content, solicitation of goods or services, abusive behavior, or offline harm.

Tinder's web-based form reporting mechanism permits both users and non-users to report a Tinder user. Tinder's current web-based form reporting mechanism also has the functionality to accept submission of screenshots or other attachments.

Hinge

Permits users to report those they have matched with, or those who they haven't matched with and see in their recommendation or stack. Users can access in-app reporting options in various screens, including when viewing their profile or after matching with them. The details provided in reports are always kept confidential in order to protect the safety and identity of the reporting user. The main reporting categories are fake profiles, scams, inappropriate content, underage users, or content that makes a Hinge user feel unsafe. Hinge also permits users and non-users to make reports via email.

Reporting someone for a discriminatory reason — such as their (actual or perceived) gender identity, gender expression, race, color, religion, or disability is not allowed on Hinge. Deliberate false reports may result in a warning or account ban.

meetic

Permits users to report other users from profile or direct messaging screens. Users can report someone prior to, or after, matching. The details provided in reports are always kept confidential in order to protect the safety and identity of the reporting user. The main reporting categories offered are "the person doesn't match their profile picture or description," scam, inappropriate behavior (on- or off-platform), harassment, underage users, and other (with a free text field). Meetic also permits users and non-users to report any safety matter, as well as illegal content, via web-based forms.

azar

Permits users to report in various ways, including during a live match, from a specific direct message, and from the profile of the user that they wish to report. The main categories available to users are (i) from a live match session: inappropriate messages, inappropriate behavior, underage user, and inappropriate video; (ii) from a direct message: sexually explicit content, fraud and spam, offensive messages, and fake profile; and (iii) from a user'sprofile: inappropriate profile photo, inappropriate profile video, inappropriate bio and nickname, underage user, other/inappropriate, and illegal content report.

okcupid

Permits users to report in various ways, including through their message list, on a specific message, on a photo, or from the profile of the user that they wish to report — regardless of if they matched with that user or not. The main categories available to users are (i) non-photo reports, which include scam or fake accounts, inappropriate messages or profiles, persons in an unsafe situation, or underage users; and (ii) photo reports, which include scam or fake accounts, inappropriate photos, nudity or sexual photos, or underage users (among other things).

OkCupid's web-based form reporting mechanism permits both users and non-users to report an OkCupid user who is engaging in unsafe behavior. OkCupid's current web-based form also has the functionality to accept submission of screenshots or other attachments. OkCupid also permits users and non-users to make reports via email.

Plenty of Fish

Permits users to report other users through their profile or based on a photo, regardless of matching with the user or not. The main reporting categories available are underage users, nudity or sexual content, solicitation of goods or services, abusive behavior, or offline harm.

Plenty of Fish's web-based form reporting mechanism permits both users and non-users to report a user who is engaging in unsafe behavior. In addition to the in-app and web-based form, Plenty of Fish also provides users and non-users with access to live chat support on the Plenty of Fish website.