[redacted]

October 9, 2023

**SENATO DELLA REPUBBLICA ITALIANA**
Piazza Madama
00186 Rome
Italy

**To the kind attention of the honourable members of the Constitutional Affairs Commission and Justice Commission**

**Re: *Atto Senato No. 878 - Draft Law for The Conversion Into Law Of Law-Decree No. 123 Of 15 September 2023 - Aylo's Position Paper On Online Minors' Protection And Safeguard Measures***

Dear Honourable Members,

We would like to express our commitment to trust and safety and our interest in the provisions set forth under Law-Decree No. 123 of 15 September 2023 ("**Law-Decree**"), which is debated under this Commission as part of its validation procedure. We feel very close with the issues raised in the Decree, such as the fight against youth disaffection as well as child safety in the digital environment.

In this brief submission, we hope to assure you that as the operator of one of the world's most well-known adults-only social media platforms, we are fully committed to the trust and safety of the public including minors, including minors – as well as of our users, partners, and our over 1,400 employees and their families.

## 1. ABOUT AYLO

First of all we would like to introduce ourselves and to make clear our main objectives. Our team includes designers, engineers, analysts, developers, editors, marketers, and legal and compliance professionals. We share a drive for excellence working alongside the brightest in our fields.

Aylo has built a successful technology company with the help of our highly skilled employees and one of the most engaged and inclusive adult audiences online. Our platforms allow consenting adults to explore content that adheres to our core values: consent, freedom of sexual expression, authenticity, originality, and diversity. In line with our values and our business model, as reflected in our terms of service and content policies, we have a zero-tolerance policy against any type of illegal content, and in particular child sexual abuse material and non-consensual content have no place on our platforms. As we will explain, Aylo is continually enhancing its trust and safety measures to combat illegal content on the Internet. The significant steps we have been taking for many years, and are constantly continuing to develop further, have set a high bar for trust and safety, not just in the adult industry, but in the entire online tech sector. Every

online platform has the moral responsibility to join this fight, and it requires collective action and constant vigilance.

## 2. BUSINESS LINES

Aylo's businesses are similar in technology to mainstream online platforms. Our primary businesses are both free and subscription video streaming sites on which we sell advertising and collect membership fees. Aylo's main business units are the following: Video Sharing Platforms (VSP), Pay Sites, Model Content Platforms, Ad Platforms and Videogame Platforms.

### 2.1. Video Sharing Platforms (including Pornhub and Youporn)

Our flagship video streaming platform is Pornhub.com. Launched in 2007, Pornhub is a leading free, ad-supported adult content hosting and streaming website that allows visitors to view content uploaded by verified Models and third-party adult entertainment companies.

Video sharing platforms allow for the general, free viewing of adult-oriented content by users, registered and unregistered. They also allow for uploading of adult-oriented content by ID-Verified Models and Content Partners. All content is moderated by nearly a dozen automated tools and is subjected to human moderator review and approval before it is published.

Other examples of our video sharing platforms are Youporn.com, Redutbe.com, and Tube8.com

### 2.2. Pay Sites (including Brazzers)

Pay sites are subscription-based platforms accessible to registered, paying members only. There is no user-generated content on Pay Sites and all content is owned or licensed by Aylo, with no interaction between users. The content is professionally produced in compliance with applicable laws, including strict age and consent record keeping requirements. In this business model, the source of revenue corresponds to user subscriptions.

Examples of our Pay Sites are Brazzers.com, Realitykings.com, Men.com, Twistys.com, Mofos.com, Transangels.com, HentaiPros.com

### 2.3. Model Content Platforms (including MyDirtyHobby)

We also have in our portfolio MyDirtyHobby, which is an online adult social network platform which allows models to interact with users. It has a European audience, with most users located in Germany. The website (and content) is accessible to registered members only. Similar to the VSP, the content is sourced from ID-verified Models and is moderated by the same automated tools and human moderation before publishing. MyDirtyHobby also includes a live streaming platform for verified models, with 24/7 human moderation of all live streams. Our source of


Licensing IP International Sarl
32, Boulevard Royal, L-2449 Luxembourg
Société à responsabilité limitée with Share Capital : USD142,178.35
R.C.S. Luxembourg: B 181 337
Tel: +352.20880.916

revenue for MyDirtyHobby are tokens/credits and subscriptions. Users may interact with Models on the platform.

### 2.4. Videogame Platform (NUTAKU)

This platform allows use, purchase, or download of its Free-to-Play or Premium Games. Registered members can view and play the games and there is no user-generated content, or interaction between users. Games are developed by third-party developers and undergo thorough review by Aylo moderators prior to being published on the platform. Our source of revenue in relation to NUTAKU are the in-game purchases through tokens/credits, premium games, and subscriptions.

### 2.5. Ad platform (TrafficJunky)

Our TrafficJunky ad platform is an ad network that manages the advertisements appearing on video sharing platform websites. TrafficJunky uses a self-serve bidding, pre-paid advertising platform to provide ad space to advertisers. The ads intermediated by TrafficJunky undergo scanning by automated tools and human moderation prior to publishing, and there is no user generated content or interactions between users on its site.

## 3. AYLO'S COMMITMENT TO SAFETY

The Aylo team and all Aylo platforms operate with Trust and Safety at the forefront of everything we do. Our goal is to achieve and set the highest level of Trust and Safety standards. This relies heavily on not only our internal policies and moderation team, but also on our array of external partnerships and technology.

As we will explain in more detail below, Aylo has a zero-tolerance policy for non-consensual content (NCC) and child sexual abuse material (CSAM). It is contrary to our values, the expectations of our employees and partners, and our business. Only by earning the trust and respect of our stakeholders and the public we can continue to be one of the world's most well-known and popular adult entertainment companies.

We have instituted some of the most comprehensive safeguards in user-generated platform history to prevent and eliminate illegal material from our site. This includes mandatory uploader verification, banning downloads of free content, expanded moderation workforce and processes, partnering with dozens of non-profit organizations in 35 countries around the world through our Trusted Flagger Program, and our Content Removal Request Form.

We are constantly improving our Trust and Safety policies to better identify, flag, remove, review, and report illegal or abusive material. We are committed to doing all that we can to ensure a safe online experience for our users, which involves a concerted effort to innovate and


Licensing IP International Sarl
32, Boulevard Royal, L-2449 Luxembourg
Société à responsabilité limitée with Share Capital : USD142,178.35
R.C.S. Luxembourg: B 181 337
Tel: +352.20880.916

always striving to do more. Aylo moderates more forcefully, swiftly, and effectively than many other popular platforms, both inside and outside the adult space.

## 4. AYLO'S CONTENT CONTROLS

Aylo has put in place many content controls mechanisms and procedures, as follows.

### 4.1. User-generated content

In December 2020, Aylo disabled all free and member access to user-generated content from all unverified user accounts. Since then, only professional studios and models who have submitted a government issued ID and passed a liveness test, verified by a third-party identification company, can upload content. We were one of the first major online platforms - adult and mainstream - to adopt this policy. This voluntary adoption of personal user verification for all active users – *i.e.*, those that upload content - is a fundamental change in the way online platforms operate. It is our hope and expectation that the entire industry will follow our lead.

### 4.2. Banned terms

Aylo has restrictions on how visitors can interact on our websites. To prevent visitors from searching for content that may violate our terms of service, we maintain a list of over 34,000 banned search terms in multiple languages. Beyond search, banned terms can also not be used in any other user-submitted text fields, such as titles, descriptions, tags, and comments.

### 4.3. Technological moderation

Our human moderators are supported by an expanding suite of technical tools including:

- Hashing technology to detect known CSAM and non-consensual content using hash-lists provided by several organisations such as the Internet Watch Foundation and STOPNCII.org
- Three layers of artificial intelligence tools to detect unknown CSAM.
- Contextual text moderation which scans comments for multiple bad behaviours
- Fingerprinting tools that ensure previously moderated and removed material cannot be re-uploaded. Our patented technology uses proprietary perceptual hashing to detect re-uploads of previously banned material, even if it has been manipulated to circumvent our moderation measures.

Overall, our tools include YouTube's CSAI Match, Microsoft's Photo DNA, Thorn's Safer, Google's Content Safety API, Spectrum Lab's text moderation, Vobile's Mediawise and Alyo's patented


Licensing IP International Sarl
32, Boulevard Royal, L-2449 Luxembourg
Société à responsabilité limitée with Share Capital : USD142,178.35
R.C.S. Luxembourg: B 181 337
Tel: +352.20880.916

technology, Safeguard. We take immediate action against any items that are detected as CSAM or non-consensual by any of our tools, and against the responsible uploaders. Our artificial intelligence tools use machine learning to detect content which could include anyone who may be under 18 to forewarn our moderators and assist them in proactively preventing the material from being published on our platforms. ''

### 4.4. Reporting

In 2020, we launched our Trusted Flagger programme. Today, this initiative enables over 55 non-profit organisations who specialize in CSAM and NCC prevention, to alert us to content that they believe may be in violation of our Terms of Service. We immediately take all appropriate and necessary action, which includes human review in all cases, against any content identified by a Trusted Flagger. Our Trusted Flaggers also have direct access to Aylo's moderation team.

Users (visitors to the platform) can also report content that violates our Terms of Service by filling out our Content Removal Request (CRR) form. Again, we take all appropriate and necessary action against reported content, which is subject to human review in all cases. Users may also alert us to potentially violating and illegal material by using our content, user and comment flagging features. All reports are kept confidential, and we review all content that is brought to our attention. Furthermore, any requests from law enforcement will be handled specifically by our legal team and we have developed a law enforcement portal to streamline this process.

### 4.5. CSAM Procedure

All content that is identified by Aylo as potential CSAM is subject to our CSAM handling and reporting process.

We will immediately deactivate and ban any user account that uploads CSAM and report the user and any content to the National Centre for Missing and Exploited Children (NCMEC). The offending user's history of interaction with our platforms is also reviewed, as is any other content the user uploads.

Any CSAM identified in this process is fingerprinted using Aylo's fingerprinting tools to prevent it being uploaded to our platforms even if it has been manipulated before re-upload.

Our transparency reports are a critical function of open communications and include a detailed breakdown of statistics on moderated and removed material. Previously annual, we began twice yearly reporting this year and all reports can be found in Pornhub's Trust & Safety Centre.



Licensing IP International Sarl
32, Boulevard Royal, L-2449 Luxembourg
Société à responsabilité limitée with Share Capital : USD142,178.35
R.C.S. Luxembourg: B 181 337
Tel: +352.20880.916

[redacted]

### 4.6. Our efforts against non-consensual content

Pornhub is an adult content-hosting and sharing platform for consenting adult use only. We have a zero-tolerance policy against non-consensual content (NCC). Non-consensual content not only encompasses NCII (Non-consensual Intimate Images, commonly referred to as "revenge pornography" or image-based abuse), but also includes any content which involves non-consensual act(s), the recording of sexual material without consent of the person(s) featured, or any content which uses a person's likeness without their consent, e.g. deepfakes.

We are steadfast in our commitment to protecting the safety of our users and the integrity of our platform; we stand with all victims of non-consensual content.

## 5. OUR FIRST OBSERVATION IN RELATION TO THE LAW-DECREE: IN GENERAL TERMS, FILTERING MEASURES AND PARENTAL CONTROL APPS CAN BE EFFECTIVE, BUT NEED TO BE DISCUSSED WITH ALL RELEVANT STAKEHOLDERS.

### 5.1. We support easy access and better conditions for parental control systems rather than age gating

We do not accept and tolerate minors on our sites under any circumstances..

We have been publicly supportive of effective processes and techniques of age verification for years and have always stated our concern with age verification to be that it must effectively protect children and ensure user safety and privacy.

Our experience in complying with age verification requirements in other jurisdictions such as the state of Louisiana in the USA, clearly shows that platform-level age verification does not work to protect children online. Also, those seeking adult content who understandably do not wish to share their personally identifiable information to age verify, will inevitably end up on irresponsible sites that don't enforce safety, privacy, consent, or content moderation. The privacy risks of age verification were also highlighted recently by the Australian government who decided not to proceed with mandatory age verification as such technology is still in its infancy. It is important to note that platform-level age verification not only does not prevent minors from accessing adult material online, but it even results in various negative consequences - by requiring adults to repeatedly provide ID or other personally identifiable information to potentially hundreds or thousands of websites, also exposes adults to the risk of identity theft, private data hacks, and extortion.

Many parental control systems already exist, such as filtering inappropriate content, regulating usage, and monitoring activity. To ensure that parental control systems that rely on filtering function effectively, providers of sexually explicit content might be required to implement technical modifications to their websites to best support such parental control systems. In


Licensing IP International Sarl
32, Boulevard Royal, L-2449 Luxembourg
Société à responsabilité limitée with Share Capital : USD142,178.35
R.C.S. Luxembourg: B 181 337
Tel: +352.20880.916

particular, providers might have to implement the "RTA" label ("Restricted to Adults"). An RTA label allows blocking a website from minors' access via a filter program. Embedding code in the page header meta tags enables filtering via web browsers, ISPs, firewall/proxy servers, plugins, toolbars, commercial filtering software, and operating systems. For example, a filter program is a standard feature in Windows. Websites with such an RTA label are not accessible to minors once the filter is activated. The RTA cannot be bypassed because it is part of the website URL. Labeling helps protect children from viewing age-inappropriate content online - as long as parents make sure to activate the featured parental controls. While this provides some protection for children, it is not the most effective solution.

If robust controls are desired then the best and most effective solution for protecting children and adults alike is to identify users once and at the source: by their device, or by their account on the device, and allow access to any age-restricted materials and websites globally based on that identification. This means users would only get verified once, through their operating system, not on each age-restricted site. This dramatically reduces privacy risks and creates a very simple process for regulators to enforce and users to follow: over 95% of devices worldwide are powered by operating systems owned by three companies.

When age verification is conducted once, on the device, by companies such as operating system developers and device manufacturers, who already hold personal data on their users, users are not encouraged to share their personally identifiable information multiple times across many different sites.

Device-level age verification also means that adult sites can be blocked from minor's devices by default, there is no reliance on platforms to comply, and no need for individual enforcement against thousands of individual sites – thus making for much more effective and cost and resource efficient enforcement. Finally there is also no risk of displacing traffic by pushing users who shy away from disclosing their personal information for the purpose of accessing an individual website from the compliant sites to less safe and non-compliant sites.

The adult industry, NGOs, and Law Enforcement have shown support for such effective device-level age verification measures, and such a solution is fit for purpose globally, ensuring an immediate effect upon software update roll-out by operating systems and device manufacturers.

### 5.2. Support parents with digital education

Technical measures alone are hardly ever sufficient to solve societal questions. Appropriate and effective protection of minors will never work meaningfully without the participation of parents. For this to happen, parents must first be able to participate in meaningful ways. Various studies show that parents do not know enough about the ways to protect their children's rights online. Parents should be educated as comprehensively as possible about the typical behavior of children and teenagers on the Internet. In particular, they should be made aware of how their


Licensing IP International Sarl
32, Boulevard Royal, L-2449 Luxembourg
Société à responsabilité limitée with Share Capital : USD142,178.35
R.C.S. Luxembourg: B 181 337
Tel: +352.20880.916

children use the Internet and what dangers and opportunities are there for their children. Parents could better supervise their children's online behavior by better digital education. We appreciate any commitment in the Law-Decree that is aimed at enhancing parents' education in this respect.

### 5.3. Technical parental control measures

In the current environment, parents can better use highly effective parental control systems such as filters with this greater awareness. This way, minors can be protected by design since the filters start at the root of the internet, unlike age verification systems. Parents could configure the router settings to filter certain content by design with that knowledge. The DNS settings in the relevant router must be changed so that the router relies on a "minor save" DNS Server. It also blocks proxy and VPN domains that bypass the filters. Mixed content sites (like Reddit and Imgur) are also blocked. Google, Bing, Yandex, DuckDuckGo, and YouTube are set to the Safe Mode. A filter software can mean software installed on the end user's device to detect and filter content unsuitable for minors. Most of these measures do not require any advanced technical skills, special protection devices, or purchased software; they can be set up quickly and easily on (almost) any device. The filter software checks whether the content accessed is appropriate for the age group in the background. Accordingly, the websites are displayed or blocked by the software.

Accordingly, it is clear that filtering measures and parental control apps can be effective, but these need to be properly addressed. Nevertheless, a good legislation should only lay down general criteria and leave it to the competent authority, in this case for the time being identified in AGCOM, to assess, together with all stakeholders, including expert platforms in the sector, which instruments are the most appropriate, in a balancing act between protection and market requirements and the free expression of thought and sexuality. The Law-Decree, as amended and converted into law at the end of this legislative procedure, should not impose precise and rigid criteria as these could be overtaken over time.

## 6. OUR SECOND OBSERVATION IN RELATION TO THE LAW-DECREE AND THE ON-GOING DISCUSSION: AGE GATING IS NOT THE CORRECT MEASURE TO PURSUE MINOR PROTECTION.

We know there is an on-going debate in Italy regarding the possibility to introduce an obligation to include age gating mechanism on certain online platforms. We hereby provide accurate information explaining why age gating is not the correct measure to pursue minor protection.



Licensing IP International Sarl
32, Boulevard Royal, L-2449 Luxembourg
Société à responsabilité limitée with Share Capital : USD142,178.35
R.C.S. Luxembourg: B 181 337
Tel: +352.20880.916

### 6.1. Fist risk: use of non-secure websites

Strict age verification (or hard age gating) systems are characterized by the fact that they require some sort of identity certification – thus revealing directly or indirectly the user's identity to the platform, or at least to a third-party registration site (linked to the use of the platform).

In the event that a strict age verification system is implemented on a specific platform for sexually explicit content, hardly any user (completely irrespective of age) will continue to visit this site. They will simply switch to other sites which do not require age verification and will typically be less compliant and subject to – often significantly – lower trust and safety measures and content moderation. Given the availability of an immense number of such other sites (without any age verification and age gating), such implementation on a limited number of individual sites is simply like a drop in the ocean. The intended protective effect is zero as users will simply move on to the less protected and non-compliant sites. Those users that – for whatever reason – do not want to move on to other sites will use methods to circumvent the age gating requirements. The latter can be easily done by VPN or Tor technologies. More tech-prone users can also use other circumvention tools such as facial morphism that allows to make one's own face more senior for the purpose of an only interview or an automatic AI screening. In this context, it is also noteworthy that anybody, including minors, pushed towards using Tor will by necessity end up in the so-called dark web. Once there, they are very likely to be exposed to illegal and extreme content they otherwise would never have come into contact with. The negative social consequences are significant and completely unacceptable – whilst being entirely avoidable through implementing controls at the device level. Moderated and compliant sexually explicit content could also help older teenagers to serve their development needs and explore their sexuality, particularly in the case of the LGBT+ community.

### 6.2. Second risk: the harm identity verification systems causes and the legitimate interest of video-sharing platform providers

As shown above, the interests of minors are not positively impacted in any relevant way by implementing age verification systems. This is because the level and amount of consumption of sexually explicit content by minors are not at all affected by any such measures, and on the contrary, minors will be incentivized to move to harmful less and non-compliant sites.

Furthermore, in direct contrast to the lack of any positive effects on the protection of minors, the legitimate interests of video-sharing platform providers would be negatively affected in the extreme. Any request to implement an identity certification requirement on their platform would lead inevitably to an almost complete loss of visitors of that platform as they would simply move on. Accordingly, the very existence of their platform would be destroyed as they would have hardly any chance of surviving the complete loss of traffic on their platform.



Licensing IP International Sarl
32, Boulevard Royal, L-2449 Luxembourg
Société à responsabilité limitée with Share Capital : USD142,178.35
R.C.S. Luxembourg: B 181 337
Tel: +352.20880.916

The result would be an absurd outcome contrary to the fundamental constitutional rights and freedoms of all parties concerned: minors would not be protected, and, at the same time, platform providers that implement strict access requirements would be wiped out from the market. This scenario would amount to an unjustified expropriation, as the singled-out provider(s) would be deprived of their commercial existence without any corresponding useful benefit for minors whatsoever.

The introduction of identity age verification systems to protect minors should also be determined in the light of the interests of the website users and the general public interest. Identity certification and age verification systems, particularly AI-based approaches such as facial recognition technologies, could easily adversely affect data protection rights and principles.

According to Art. 5 (1) lit. c of the General Data Privacy Regulation (GDPR), personal data must be processed in a way that is adequate, relevant, and limited to what is necessary for the purposes for which they are processed. The nature of identity certification systems to check someone's age is to collect detailed, sensible data. Art. 9 (1) GDPR regards all personal data related to the sexual orientation of a data subject as a special category of personal data. These personal data are particularly sensitive data. As such, they are in a particular way protected by the GDPR. The requirement that data must be limited to what is necessary thus takes on additional weight in the case of sensitive personal data of special categories.

AI approaches collect users' personal biometric data (Art. 9 (1) GDPR). In particular, they take and save images of the user's face, creating a biometric template of it.

Given the complete lack of proven benefits of identity certification systems and strict age verification / hard are gating at website level, it is neither adequate nor relevant nor necessary within the meaning of Art. 5 GDPR to collect and store the visitor's personal data, potentially every time a user visits a different adult content website. This goes all the more as these data are highly sensitive – as they relate to the consumption of sexually explicit content by an individual.

In addition, the identification of the visitor may allow the creation of personalized "user profiles" that trace, track, analyze and store each user's consumption habits of sexually explicit content. It is difficult to imagine any personal data that would be more worthy of protecting.

Users who use websites with sexually explicit content are highly interested in informational self-determination. Data collected about their usage behavior affects their most intimate sphere of personality rights, encompassing their sexual orientation and sexual preferences. If such data become public, this could have significant consequences for their family, social sphere, and professional lives. Identifying certification systems can cause substantial harm to the right of informational self-determination of website users. The data collected via such systems significantly increases the risk of hacking such data. Furthermore, the risk of hacks of identity certification systems particularly affects vulnerable groups such as the LGBT+ community.



Licensing IP International Sarl
32, Boulevard Royal, L-2449 Luxembourg
Société à responsabilité limitée with Share Capital : USD142,178.35
R.C.S. Luxembourg: B 181 337
Tel: +352.20880.916

Summed up, Identity certification and age verification systems at website level are no proportionate measures in the light of the amount of risk they create and harm they cause both to affected users and to the commercial livelihood of video-sharing platform providers. They would also by necessity be applied in an arbitrary and unequal manner – because they cannot be realistically enforced on all relevant websites that are out there. They lead to a de facto expropriation and violate other fundamental rights under the EU Charter on Fundament Rights. At the same time, they are also not serving any interests of website users, be they minors or adults. On the contrary, they would result in significant harm, run foul of data protection principles, and embody a tremendous risk for the right to informational self-determination of the website users by creating unnecessary hacking risks for the large amount of highly sensitive personal user data that would need to be collected.

## 7. THIRD OBSERVATION IN RELATION TO THE LAW-DECREE: ITS CURRENT TEXT MUST BE REVIEWED SO AS TO CLARIFY ONLINE PLAYERS' ROLE AND DEFINITIONS

Finally, we would like to point out the need to clarify certain aspects of the text of the Law-Decree, particularly with regard to its scope and definitions. Indeed, many aspects remain open, such as the definitions of "device" and "applications", which are so broad as to include within the definition of "device", for example, any "Internet of Things" device. In addition, there is no definition of an electronic communications service, and coordination with other legislation may lead to friction in the actual interpretation of the Law-Decree. In this respect, we believe that the text should be revised to better clarify its purpose, which, at least in its rationale, should be limited to companies providing telecommunications services and device manufacturers (as mentioned, to be better defined).



Licensing IP International Sarl
32, Boulevard Royal, L-2449 Luxembourg
Société à responsabilité limitée with Share Capital : USD142,178.35
R.C.S. Luxembourg: B 181 337
Tel: +352.20880.916

[redacted]

## 8. CONCLUSIONS

We welcome this opportunity to discuss the critical value of protecting minors in the online context as well as Aylo's unwavering commitment to trust and safety, including our work to eradicate CSAM and non-consensual material across all our platforms and across the wider internet. We are proud to be a leader in this effort, not only among adult entertainment platforms, but also among our peers in the online landscape. Our commitment to trust and safety is vital to our employees, partners, community members and the public at large, as well as to our mission to become the world's most trusted and most popular adult entertainment company.

Sincerely,

**AYLO HOLDINGS S.À R.L.**

[redacted]

By: Andreas Alkiviades Andreou
Title: Manager Class A

[redacted]

By: Anis Baba
Title: Manager Class A



Licensing IP International Sarl
32, Boulevard Royal, L-2449 Luxembourg
Société à responsabilité limitée with Share Capital : USD142,178.35
R.C.S. Luxembourg: B 181 337
Tel: +352.20880.916

## Natale, Valerio

**From:** David Cooke [redacted]
**Sent:** 09 October 2023 10:47
**To:** Natale, Valerio
**Subject:** Aylo Position Paper
**Attachments:** Aylo - Position Paper.pdf

**[EXTERNAL]**
Dear Valerio,

The undersigned Andreas Andreu, Manager Class A, and Anis Baba, Manager Class A, hereby authorises Attorney Valerio Natale to file the attached position paper on behalf of Aylo Holdings S.A.R.L. before the Camera dei Deputati and Senato della Repubblica. This document can be published on institutional websites

Kind regards,
David Cooke
**Sr. Director, Trust & Safety Regulations & Partnerships**
[redacted]