The EU Digital Euro project, with its emphasis on privacy and user control, **potentially offers a more reliable payment alternative for sensitive transactions**, including those for adult content. Its offline functionality and tiered privacy model could reduce data exposure compared to current private payment processors. However, **it is unlikely to completely solve issues like "definitional creep" or payment processor influence**, as Payment Service Providers (PSPs) will still handle onboarding and compliance, and broader regulatory frameworks like the Digital Services Act (DSA) will continue to shape platform content policies. The digital euro's success in this area will depend on its final design, the regulatory environment for PSPs, and its ability to provide a genuinely neutral payment rail.

# EU Digital Euro and Payments for Adult Content: An Analysis

## 1. The EU Digital Euro: Technical Design and Privacy for Sensitive Payments

### 1.1. Privacy Features of the Digital Euro

The European Central Bank (ECB) has emphasized that **privacy is a cornerstone of the digital euro's design**, aiming to offer the highest privacy standards among electronic payment options . This commitment stems from public demand, with a significant portion of respondents in a public consultation (43%) prioritizing privacy and data protection . The ECB's approach involves **"privacy by design,"** integrating data protection from the outset through technological innovation, a robust legal framework, and stringent compliance procedures . For online transactions, the Eurosystem intends to implement measures ensuring it **cannot directly link transactions to specific individuals** . This is a critical distinction from many current private digital payment solutions where providers can collect extensive data on users and their transactions . The ECB asserts that the digital euro, as a public good, **will not utilize user data for commercial purposes**, a significant departure from the practices of many private payment processors . This focus on privacy is not only a response to user preferences but also a recognition of privacy as a fundamental right under the EU Charter of Fundamental Rights (Articles 7 and 8) .

The technical implementation of privacy involves several layers. The Eurosystem plans to use **state-of-the-art measures such as pseudonymisation, hashing, and data encryption** to prevent the direct linkage of digital euro transactions to specific users . This means that while intermediaries (like banks) will have access to necessary personal data for compliance with EU law (e.g., Anti-Money Laundering regulations),

the central bank itself will not have this direct identifying information . The **separation of a user's digital euro identity from their payment data** is a key technological measure, ensuring the Eurosystem processes a minimal amount of data . Furthermore, the ECB has committed to being supervised by independent data protection authorities to ensure compliance with EU data protection laws, including the General Data Protection Regulation (GDPR) and the European Union Data Protection Regulation (EUDPR) . This multi-faceted approach—combining technological safeguards, strict rules, and independent oversight—aims to build trust and ensure the digital euro respects user privacy while meeting regulatory obligations. The design also includes an **"opt-in" mechanism for allowing PSPs to process a user's personal data for commercial purposes**, ensuring users have control over their data beyond what is necessary for legal compliance .

### 1.2. Offline Functionality and Cash-Like Privacy

A significant privacy-enhancing feature of the digital euro is its planned **offline functionality, designed to offer a level of privacy comparable to cash transactions** . This feature is particularly relevant for sensitive payments, as it would allow users to make payments without an internet connection, with transaction details known only to the payer and the payee . Such offline transactions would **not be shared with payment service providers, the Eurosystem, or any supporting service providers**, mirroring the anonymity of physical cash exchanges . The European Data Protection Board (EDPB) and national data protection authorities like France's CNIL have strongly advocated for the prioritization of this offline electronic wallet feature, emphasizing its importance for peer-to-peer payments and mitigating risks of generalized transaction tracing . The CNIL specifically recommended that **offline functionality should be available from the launch of the digital euro**, not introduced as a secondary step .

The cash-like privacy offered by the offline digital euro is a direct response to concerns about the increasing digitization of payments leading to less privacy by default . While online payments will still be subject to certain controls, the offline mode aims to preserve the anonymity that many users value, especially for low-value, everyday transactions. However, to manage risks associated with illicit activities, **full privacy in offline mode is anticipated only for close-proximity payments that are low-value and low-risk** . This balance attempts to reconcile the desire for privacy with the need to prevent financial crime. The development of an "offline digital euro device," a combination of hardware and software, will enable users to store offline holdings and conduct these private transactions . The introduction of such a feature could provide a

crucial payment alternative for individuals and businesses dealing in sensitive goods or services, who may otherwise face deplatforming or scrutiny from traditional payment processors. The ECB has indicated that for offline transactions, **no personal data would be collected**, aligning with the treatment of cash under AML/CFT regulations for low-value e-money products .

### 1.3. Pseudonymisation and Data Encryption

To safeguard user data in online digital euro transactions, the Eurosystem will employ advanced privacy-enhancing technologies, including **pseudonymisation, hashing, and data encryption** . Pseudonymisation is a key technique where directly identifiable information (like a user's name) is replaced with a random, unique identifier (a pseudonym) . This means that while the user's bank or payment service provider (PSP) will have access to the personal data necessary for compliance with regulations such as Anti-Money Laundering (AML) and Counter-Terrorism Financing (CFT), **the Eurosystem itself will not be able to directly link transactions to specific, identifiable individuals** . The data available to the Eurosystem will be pseudonymised, ensuring that no personal data that could identify a user is visible to the central authority . This separation of identity from transaction data is a fundamental aspect of the digital euro's privacy architecture . An "alias," such as a unique digital euro account number (DEAN), will be used as a pseudonymous identifier to protect a user's identity during payment processing, and this alias can only be attributed to an identifiable person by the distributing PSP or the user themselves, not by the Eurosystem during settlement .

Data encryption will further protect the confidentiality and integrity of transaction data, both in transit and at rest. While specific encryption algorithms are not detailed, the commitment to "state-of-the-art measures" suggests the use of robust, industry-standard cryptographic techniques . The ECB has also stated its commitment to continuously assess new privacy-enhancing technologies that might become feasible and effective . These technical measures are complemented by strong contractual safeguards, IT security rules, and audit rights for service providers, ensuring that privacy and data protection standards are rigorously enforced throughout the digital euro ecosystem . The combination of these technologies aims to provide a **higher level of privacy for online digital euro payments compared to many existing commercial digital payment solutions**, where data collection for commercial purposes is common . This approach seeks to build user trust by ensuring that financial activities remain private and that the Eurosystem does not track individual payment patterns .

### 1.4. Tiered Privacy and Transaction Limits

The digital euro is designed with a **tiered approach to privacy**, acknowledging the need to balance user privacy with regulatory requirements, particularly concerning Anti-Money Laundering (AML) and Counter-Terrorism Financing (CFT) . The baseline scenario for online transactions involves transparency to intermediaries (e.g., banks or PSPs), who would have access to personal and transaction data to ensure compliance with AML/CFT regulations, similar to current private digital payment solutions . This means customer checks during onboarding (Know Your Customer – KYC procedures) and ongoing monitoring of transactions by these intermediaries. However, the Eurosystem itself aims to see only the minimum transaction data required to validate payments, even if it performs the settlement function . Beyond this baseline, the ECB is exploring options for enhanced privacy, particularly for low-value payments. One such option is **"selective privacy" for low-value/low-risk transactions**, which might involve simplified checks during onboarding, potentially through specific wallets with lower requirements . This could offer a higher degree of privacy for everyday small purchases. Higher-value transactions would, however, remain subject to standard controls .

The most significant enhancement is the **offline functionality, which promises cash-like privacy for low-value, close-proximity payments**, where neither the intermediary nor the central bank would know the transaction details or balances . The EDPB and CNIL have also suggested implementing a "privacy threshold" for both online and offline use, below which transaction data would remain on the user's device and not be traced . Additionally, **holding limits for digital euros are being considered** to prevent its use primarily as a store of value and to maintain financial stability, which could also interact with privacy features . Proposed holding limits for individuals range from **€3,000 to €5,000** . If a user's digital euro balance exceeds this limit, mechanisms like "defunding" or a "waterfall functionality" would automatically transfer the excess amount to a linked private bank account . For offline transactions, specific limits are also anticipated, potentially aligned with existing AML/CFT exemptions for low-value e-money (e.g., **€150 for face-to-face, €50 for remote**) . The concept of "anonymity vouchers" has also been mentioned, allowing users to anonymously transfer a limited amount of digital euros over a defined period, though this would likely only apply to small transactions and protect identity vis-à-vis the central bank, not necessarily the PSP .

### 1.5. Potential for a Reliable Alternative for Sensitive Transactions

The EU Digital Euro, particularly with its offline functionality and enhanced privacy features for online transactions, **holds the potential to offer a more reliable payment alternative for individuals and businesses involved in legally permissible but sensitive activities**, such as sex work, erotic game development, or adult content creation. The cash-like privacy of offline transactions could be particularly beneficial, as it would allow payments to occur without revealing sensitive data to intermediaries or the central authority . This could mitigate the risk of deplatforming or financial censorship that these groups often face from traditional payment processors, who may have restrictive policies or be influenced by broader regulatory pressures and societal stigma . For online transactions, while intermediaries will have some access to data for AML/CFT compliance, the Eurosystem's commitment to not directly linking transactions to individuals and not using data for commercial purposes could provide a greater degree of confidence than current commercial payment solutions . The fact that the digital euro is intended to be **legal tender** could also reduce the ability of intermediaries to arbitrarily deny service to legal businesses .

However, the extent to which the Digital Euro becomes a truly reliable alternative depends on several factors. Firstly, the **final design of the privacy features, especially the thresholds for low-value transactions and the specifics of the offline mode, will be crucial** . If these are too restrictive, they may not be practical for all transactions. Secondly, the **role and obligations of Payment Service Providers (PSPs) in the digital euro ecosystem will be significant**. While the ECB aims for high privacy standards, PSPs will still be responsible for onboarding and AML/CFT checks . If PSPs face pressure to overly scrutinize transactions related to adult content, or if the "definitional creep" of prohibited content extends to PSPs' interpretation of their duties, the benefits of the digital euro's privacy could be undermined at the point of user access. The success of the digital euro for sensitive transactions will also hinge on its widespread acceptance and ease of use, ensuring it is a viable option for both payers and payees in these sectors. The legislative framework will ultimately determine the balance between privacy and other policy objectives, such as preventing illicit activities .

## 2. Regulatory Framework and Legal Aspects of the Digital Euro

### 2.1. EU's Stance on Digital Regulation and User Rights

The European Union has been actively shaping its digital regulatory landscape with a **strong emphasis on protecting user rights, including privacy, data protection, and**

**consumer protection**. The development of the digital euro is situated within this broader context, aiming to provide a digital payment option that aligns with these fundamental EU values . Privacy and data protection are enshrined as fundamental rights in the Charter of Fundamental Rights of the European Union (Articles 7 and 8) , and the digital euro project is explicitly designed to uphold these rights . The ECB has stated that ensuring user privacy has been a central focus from the start, requiring not only technological innovation but also a strong legal framework and rigorous compliance procedures . This commitment is further underscored by the ECB's obligation to comply with stringent EU data protection laws like the General Data Protection Regulation (GDPR) and the EUDPR, and its supervision by independent data protection authorities . The EU's approach to digital regulation also involves fostering competition and ensuring that digital markets are fair and transparent, as seen in the Digital Services Act (DSA) and the Digital Markets Act (DMA) .

The EU's strategy also includes **promoting European technological sovereignty and reducing dependence on non-European payment providers** . The digital euro is envisioned as a pan-European payment solution operating under European governance, which could enhance the competitiveness of the European payments industry and offer an alternative to dominant international players . This regulatory environment suggests that the digital euro will be designed and governed with a keen awareness of user rights, although the precise balance with other objectives like AML/CFT compliance remains a key area of development and debate . The Digital Euro Rulebook Development Group, chaired by the ECB and including consumer organizations, is tasked with drafting the rules for the digital euro scheme, bound by the legislative framework . This contrasts with the current landscape where private payment processors often set their own rules with limited public oversight . The EU aims to ensure that the Digital Euro is designed with privacy by default and by design, reflecting the high value placed on data protection .

### 2.2. Anti-Money Laundering (AML) and Counter-Terrorism Financing (CFT) Requirements

A critical aspect of the digital euro's regulatory framework is its **adherence to Anti-Money Laundering (AML) and Counter-Terrorism Financing (CFT) regulations**. The ECB has consistently stated that while privacy is a key objective, it must be balanced with other EU policy goals, notably AML/CFT . This means that **complete anonymity, especially for larger or online transactions, is not considered a desirable feature**, as it would hinder the ability to control the amount of digital euro in circulation and prevent

illicit activities . Consequently, the digital euro design incorporates mechanisms to ensure compliance with these regulations. For online transactions, intermediaries (Payment Service Providers – PSPs like banks) will be responsible for conducting customer due diligence (CDD), including Know Your Customer (KYC) checks during onboarding, and monitoring transactions for suspicious activity . These PSPs will have access to the personal data necessary to fulfill these AML/CFT obligations .

The Eurosystem itself, while aiming not to directly link transactions to individuals, will have access to anonymised or aggregate data for statistical, research, supervisory, and oversight purposes, including fighting fraud and illicit activities . The offline functionality, which offers cash-like privacy, is also expected to have limitations to contain risks, likely being restricted to low-value, low-risk, close-proximity payments . The European Data Protection Board (EDPB) and national authorities like the CNIL have emphasized the need for a specific legal regime for the digital euro to clearly define this balance between privacy and AML/CFT requirements . This suggests that the existing AML/CFT framework will be adapted or supplemented to accommodate the unique characteristics of the digital euro. The challenge lies in designing a system that effectively combats financial crime without unduly compromising the privacy benefits the digital euro aims to offer, particularly for legitimate but sensitive transactions. The reputational risk to central banks if their digital currency systems are used for illegal transactions is also a significant consideration . The European Banking Federation (EBF) has also emphasized that commercial banks must have access to customer data to perform these regulatory checks and fraud control, and there should be the same rules for all digital payments, including CBDCs .

### 2.3. The Digital Services Act (DSA) and its Impact on Adult Content Platforms

The Digital Services Act (DSA) represents a significant piece of EU legislation with **direct implications for online platforms, including those hosting adult content**. The DSA aims to create a safer digital space by clarifying the responsibilities of online intermediaries and platforms concerning illegal content, disinformation, and the protection of fundamental rights, including the protection of minors . **Very Large Online Platforms (VLOPs)**, which include major adult content sites like Pornhub, Stripchat, and XVideos due to their large user bases (over 45 million monthly active users in the EU), are subject to stricter obligations under the DSA . These obligations include conducting thorough risk assessments related to the dissemination of illegal content, the negative effects on fundamental rights, public security, and the protection of minors . They must also implement effective risk mitigation measures, such as **robust age verification**

**systems to prevent underage access to pornographic material**, and content moderation tools . The European Commission has launched investigations into several major pornographic websites to assess their compliance with DSA provisions, particularly concerning measures to protect minors and prevent the amplification of illegal content and gender-based violence . Platforms found non-compliant risk significant fines, up to 6% of their global annual turnover .

While the DSA primarily governs the content and operational aspects of these platforms, its requirements for age verification and the handling of sensitive content could indirectly influence payment processing. If platforms are mandated to implement more stringent user verification, this could intersect with payment data. The digital euro, with its focus on privacy, might offer a payment method that aligns with the DSA's goals of user protection while minimizing data exposure. However, the DSA's emphasis on preventing access to sensitive material by minors also underscores the need for systems that can, where necessary and lawful, link transactions to verified identities for age verification purposes, which presents a complex interplay with the digital euro's privacy features. The DSA also requires VLOPs to provide transparency regarding their advertising and to grant researchers access to data, further increasing scrutiny on these platforms . The DSA's definition of "illegal content" is broad and central to its enforcement, encompassing any information or activity that does not comply with EU or national law . Platforms must act against illegal content when made aware of it but are explicitly excluded from any general monitoring obligation . The DSA also mandates transparency reporting and requires platforms to act on their own content standards diligently and proportionately, respecting fundamental rights .

### 2.4. Financial Inclusion and the Digital Euro

A key objective of the digital euro project is to **ensure financial inclusion, making it accessible to all segments of the population**, including those who may be vulnerable to digital financial exclusion . The ECB envisions the digital euro as a public good, similar to banknotes and coins, but in a digital form, and intends for basic use to be free via a mobile app or a physical card . This is supported by draft legislation from the European Commission, which proposes that credit institutions distributing the digital euro should provide basic digital euro payment services for free when requested by their customers . This approach aims to prevent the digital euro from becoming a service only accessible to or affordable for certain groups, thereby promoting broader participation in the digital economy. The **offline functionality is also a crucial component for inclusion**, as it would allow payments in areas with limited or no

internet connectivity, or for individuals who may not have consistent access to the internet .

To further support inclusion, the ECB plans to identify public entities, such as post offices, in each euro area country. These entities would provide free support and access to digital euro services for people who are vulnerable to digital financial exclusion, including those with disabilities, functional limitations, limited digital skills, and elderly people . This support could involve face-to-face assistance with opening a digital euro account and using basic services. Importantly, **free access to basic digital euro services would also be offered to individuals without a bank account**, addressing a key barrier to financial inclusion for the unbanked population . Specific attention will also be given to particularly vulnerable groups, such as individuals with no fixed address, asylum seekers, or beneficiaries of international protection . By designing the digital euro with these considerations, the ECB aims to ensure that the transition towards digital payments does not leave certain demographics behind, fostering a more inclusive digital financial ecosystem. This contrasts with some private payment solutions that may have fees or accessibility barriers for certain users or transaction types. However, concerns exist that reliance on PSPs for distribution could lead to financial exclusion if these intermediaries apply overly restrictive KYC practices .

### 2.5. Legal Tender Status and Acceptance

The digital euro is intended to be a form of central bank money, making it inherently risk-free and backed by the Eurosystem, distinguishing it from private stablecoins or crypto-assets . While the provided excerpts do not explicitly state that the digital euro will have "legal tender" status in the same absolute sense as euro banknotes and coins (which must be accepted for the settlement of debts), it is designed to be a widely accepted and accessible digital form of the single currency . The **European Commission has proposed a framework that would establish the digital euro as legal tender for online payments** within the euro area . This means that, like cash, it would have to be accepted by payees (e.g., merchants, service providers) as a means of settling a monetary debt, provided the payment is made online and the payee is established in the euro area . The ECB's aim is for the digital euro to be used for everyday payments, both online and offline, by individuals and businesses across the euro area . The draft legislation from the European Commission is a key component in establishing the framework for its issuance and use, which will define its characteristics and the obligations of various parties, including payment service providers . The goal is

to provide a **pan-European payment solution that is universally accepted within the euro area**, reducing fragmentation and reliance on non-European payment providers .

The acceptance of the digital euro will be crucial for its success. The ECB is working on ensuring it can be used for a wide range of transactions, including point-of-sale (POS) payments, online purchases, and person-to-person (P2P) transfers . For businesses, the digital euro is intended to offer a cost-effective payment solution, potentially providing competition to international card schemes and reducing transaction costs . However, some analyses suggest that many use cases for the digital euro are already covered by existing payment solutions, and it's not yet clear if the digital euro will offer superior convenience or features that would drive widespread merchant adoption beyond what is mandated or incentivized. The practical implications of legal tender status for sensitive payments mean that while merchants accepting digital payments would generally be obliged to accept the digital euro, this does not override other legal or regulatory obligations, such as those imposed by the DSA on platforms hosting adult content .

## 3. Comparison: EU Digital Euro vs. Current Payment Processor Influence

### 3.1. "Definitional Creep" and Payment Processor Influence on Adult Content

The term **"definitional creep"** describes a phenomenon where the boundaries of what constitutes prohibited or "harmful" content, particularly in the context of adult material, are progressively expanded by private financial intermediaries rather than through public, democratic legislative processes . This expansion is largely driven by the risk management strategies and brand reputation concerns of major credit card networks like Visa and Mastercard, and the payment processors that operate under their rules . These financial entities, while not public regulatory bodies, wield significant power in determining what types of sexual content can be monetized online. Their policies often prioritize a narrow, normative moral ordering of sexuality, which can lead to the censorship of diverse erotic expressions, kink, and other forms of adult content that do not align with their corporate interests or perceived mainstream acceptability . This effectively allows private financial companies to establish **de facto global obscenity standards**, bypassing legal frameworks and public discourse. The concern is that this "definitional creep" is an ongoing process, continuously broadening the scope of what is considered unacceptable, thereby restricting adult sexual autonomy and diversity under the guise of ensuring safety, consent, and legality, but often based on a misreading or misapplication of these concepts to serve corporate rather than

collective interests . The influence of these payment processors is a critical factor for platforms hosting adult content, as the threat of losing payment processing capabilities can compel them to adopt and enforce these restrictive and often vague standards.

The research by Webber and Franco (2024) highlights that payment intermediaries, particularly credit card networks and the processors that implement their policies, play a crucial role in shaping the landscape of monetized sexual content on adult platforms . These financial actors impose a moral framework on sexuality that prioritizes the protection of credit card brand reputation and optics over the autonomy and integrity of individuals producing and consuming sexual content. Visa and Mastercard, through their intermediary payment processors, often suppress kink and other forms of non-normative sexual content under the banner of ensuring consent and safety. However, this process frequently leads to an **inappropriate broadening of the definition of 'harmful' sexual content**. This "definitional creep" results in private financial entities effectively creating and enforcing de facto global obscenity laws that serve corporate interests rather than collective or individual well-being . The rules established by these financial companies and enforced by adult platforms reproduce a normative moral ordering of sexuality, enacted through a particular interpretation of safety, risk, harm, and consent that may not align with the actual experiences or rights of content creators and consumers. This corporate-driven censorship can stifle sexual expression and limit the availability of diverse adult content, impacting sex workers, developers of erotic games, and creators of pornographic material who find their work marginalized or demonetized not due to illegality, but due to the financial sector's risk aversion and moral judgments . The case of Steam, a major digital game distribution platform, illustrates this power dynamic, where Valve updated its publishing guidelines to explicitly ban games that violate the rules set by its payment processors, particularly targeting "certain kinds of adult only content" .

### 3.2. Case Study: Steam's Adult Content Policies and Payment Processor Pressure

The digital distribution platform Steam, operated by Valve, provides a clear example of how **payment processor influence can shape content policies, particularly concerning adult-oriented video games**. Reports indicate that Steam updated its adult content policies, introducing vaguer guidelines, in response to pressure from payment processors such as Visa and Mastercard . These financial institutions reportedly threatened to withdraw payment services if Steam did not comply with their standards regarding acceptable content. This pressure stems from the adult content industry being categorized as "high risk" by payment processors, primarily due to concerns

about chargebacks and fraud, rather than solely puritanical premises . The "definitional creep" concept is evident here, as payment processors enforce often ambiguous policies to manage perceived risks, leading platforms like Steam to act as de facto censors to maintain access to essential payment infrastructure . Valve explicitly stated that certain games on Steam were retired because they "may violate the rules and standards set forth by our payment processors and their related card networks and banks," emphasizing that the loss of payment methods would prevent customers from purchasing other titles on the platform . This situation underscores the significant leverage payment processors hold over online platforms, compelling them to align their content moderation with the financial sector's risk appetite and moral frameworks, even if it means adopting vague or overly restrictive rules that can stifle creative expression and limit consumer choice .

The changes in Steam's policies highlight a growing external influence over its content decisions, moving towards allowing payment services to dictate what is permissible . This shift introduces considerable ambiguity for developers, who are given little specific guidance beyond avoiding content that "may violate the rules and standards" set by payment processors, banks, or even internet network providers . The inconsistency and lack of transparency in how banks and payment processors approach adult content have long been a challenge for businesses in the adult industry, and this vagueness appears to be reflected in Steam's updated guidelines . While Valve has expressed a willingness to continue hosting adult content, the new policy effectively defers significant aspects of content moderation to these financial entities. The consequence is a **chilling effect on certain types of adult games**, particularly those with themes like incest, which have reportedly been targeted for removal . This case illustrates the power dynamics at play, where private payment processors, driven by their own risk assessments and reputational concerns, can indirectly dictate the boundaries of acceptable online content, impacting not only the platforms but also the developers and consumers within those ecosystems. The "definitional creep" ensures that these boundaries can shift without clear public accountability, as the standards are set by private corporations rather than through transparent regulatory or legislative processes. Following the policy update, several explicit games were removed from Steam, with reports indicating titles containing terms like "incest" or "slave" were among the first to be taken down .

### 3.3. The Digital Euro as a Public Payment Option vs. Private Processor Dominance

The EU Digital Euro project, as a central bank digital currency (CBDC), presents a **potential alternative to the current system dominated by private payment processors**. Unlike private payment systems, which are primarily accountable to shareholders and driven by profit motives and risk management that can lead to "definitional creep" and financial censorship , a publicly issued digital euro would, in principle, operate under a different set of objectives. The European Central Bank (ECB) has emphasized goals such as financial inclusion, ensuring access to a digital form of cash, and maintaining public money as an anchor for the payment system . The Veblen Institute's study, "A digital euro for a better monetary system," likely advocates for the Digital Euro as a public option that could address some of the shortcomings of the current financial landscape, potentially including the corporate-driven restrictions on legal but sensitive transactions . If the Digital Euro is designed to be a public good, it could offer a payment rail that is less susceptible to the moral ordering and risk-aversion of private financial institutions, thereby providing a more neutral platform for transactions, including those for adult content, provided they are legal. The success of such an approach would depend heavily on the specific design choices, particularly concerning privacy, anonymity, and the role of intermediaries in the Digital Euro ecosystem.

The current dominance of private payment processors like Visa and Mastercard in the digital payments space gives them considerable power to influence what types of legal content and businesses can access financial services . This influence often translates into de facto censorship, as seen in the Steam case, where platforms are pressured to alter content policies to avoid being cut off from payment processing . The Digital Euro, as a public infrastructure, could theoretically disrupt this dynamic by providing an alternative payment system that is not governed by the same corporate interests or risk perceptions that drive "definitional creep." The European Commission's proposal envisages the Digital Euro being distributed indirectly through financial intermediaries, including credit institutions and other payment service providers (PSPs) . While this still involves private entities in the distribution chain, the underlying currency and potentially the core infrastructure would be public. This could lead to a different set of incentives for these intermediaries compared to the current system where they are often bound by the stringent and often opaque rules of international card networks. The extent to which the Digital Euro can offer a genuinely neutral payment option will depend on the regulatory framework governing its use, the level of privacy it affords, and the degree to which PSPs are allowed or encouraged to apply their own content-based restrictions when facilitating Digital Euro transactions. The aim of fostering competition and choice in digital payments, as mentioned in ECB documents , could also indirectly benefit

sectors currently facing payment processor discrimination if the Digital Euro creates viable alternatives.

### 3.4. Potential for Reduced Corporate Censorship

The EU Digital Euro project holds the **potential to reduce corporate censorship**, particularly the kind driven by the policies of private payment processors, by offering an alternative payment infrastructure that is publicly governed and prioritizes user access and privacy within legal boundaries. Currently, platforms like Steam face significant pressure from payment processors such as Visa and Mastercard to restrict or remove certain types of content, especially adult content, due to the processors' risk assessments and terms of service . This often leads to "definitional creep," where the scope of prohibited content expands beyond what is strictly illegal, effectively allowing these private financial entities to act as arbiters of acceptable speech and commerce . The Digital Euro, as a public utility, would operate under a different set of motivations, primarily focused on providing a secure, efficient, and accessible digital payment option for all euro area citizens, rather than maximizing profit or minimizing corporate risk in the same way private companies do . If the Digital Euro can provide a reliable payment rail that is not subject to the same content-based restrictions imposed by private card networks, it could empower platforms and merchants, including those in the adult industry, to transact more freely for legal goods and services.

The design of the Digital Euro, particularly its privacy features, could further contribute to mitigating corporate censorship. The proposal includes provisions for **offline peer-to-peer transactions, which would offer a degree of anonymity similar to cash**, and tiered privacy for online transactions where the European Central Bank (ECB) would not directly access personal transaction data, leaving this to regulated Payment Service Providers (PSPs) under strict AML/CFT obligations . This contrasts with the current system where private payment processors have extensive visibility into transaction details, which they can use to enforce their content policies. Moreover, the EU's broader regulatory landscape, including the Digital Services Act (DSA), aims to ensure that online platforms operate transparently and are accountable for their content moderation decisions, while also protecting fundamental rights like freedom of expression . The DSA requires platforms to provide clear reasons for content removal or monetization restrictions and allows users to challenge these decisions . While the DSA does not prohibit platforms from having their own content standards, it does aim to curb arbitrary or opaque moderation practices. The combination of a publicly backed digital currency and a regulatory framework that emphasizes transparency and user

rights could create an environment less conducive to the kind of corporate censorship currently experienced by platforms and content creators who fall outside the narrowly defined "acceptable" content parameters of major payment processors. However, the extent of this reduction in corporate censorship will heavily depend on the final design of the Digital Euro, the specific obligations placed on PSPs, and how the DSA is enforced in practice, particularly concerning the handling of legal but sensitive content.

### 3.5. EU's Regulatory Approach vs. Industry-Led Standards (US Comparison)

The European Union's approach to digital regulation, including the development of the digital euro, contrasts significantly with the more industry-led standards often observed in the United States . The EU has established a comprehensive regulatory framework that prioritizes user rights, data protection, and market fairness, often imposing specific obligations on companies to ensure compliance. Landmark legislation like the General Data Protection Regulation (GDPR), the Digital Services Act (DSA), and the Digital Markets Act (DMA) exemplify this proactive stance, aiming to create a safer and more accountable digital environment . This regulatory philosophy means that the rules governing the digital euro, its privacy features, and the responsibilities of intermediaries (PSPs) will be heavily shaped by existing EU law, with a strong emphasis on fundamental rights and consumer protection. The EU's strategy also includes fostering European technological sovereignty and reducing reliance on non-European payment providers, which further informs its approach to developing a public digital currency .

In contrast, the United States has historically favored a more laissez-faire approach, allowing industry to develop its own standards and practices with less direct government intervention in many digital domains. While the US has regulations in areas like financial services and consumer protection, the level of prescriptive detail and enforcement in areas like data privacy and platform accountability can differ from the EU model. This difference in regulatory philosophy has implications for how issues like "definitional creep" in adult content payments are addressed. In the US, the policies of dominant private payment processors often set de facto standards without extensive public oversight, as seen with platforms like Steam being influenced by payment processor demands . The EU's more assertive regulatory stance, through instruments like the DSA and the proposed digital euro framework, aims to create a system with greater public accountability and potentially more robust protections for users and businesses against arbitrary corporate policies. The digital euro, as a public initiative, is intended to operate under clear legal frameworks that prioritize user rights and European strategic interests, potentially offering a more stable and predictable

environment compared to one solely governed by the evolving terms of service of private, often foreign, corporations.

## 4. Addressing Specific Issues: Payment Processor Influence and "Definitional Creep"

### 4.1. The Challenge of "Definitional Creep" in Adult Content Payments

The challenge of **"definitional creep" in adult content payments** refers to the phenomenon where payment processors and financial institutions progressively expand their definitions of prohibited or "high-risk" content, often extending beyond what is strictly illegal under applicable laws . This expansion creates significant uncertainty and operational difficulties for businesses operating in the adult industry, including sex workers, developers of erotic video games, and creators of pornographic material. As highlighted in the context of platforms like Steam, payment processors such as Visa and Mastercard wield considerable influence over what content can be monetized by threatening to withdraw payment services . Their terms of service and merchant guidelines often contain broad and vaguely worded prohibitions against content deemed "objectionable," "immoral," or "harmful," categories that can be subjectively interpreted and applied inconsistently . This leads to a situation where legal adult content, which may not violate any specific laws, is nonetheless denied payment processing capabilities, effectively censoring it. The problem is exacerbated by the **lack of transparency in how these definitions are formulated and enforced**, leaving businesses with little recourse or clarity on how to comply . This "definitional creep" not only impacts the financial viability of adult content creators but also has a chilling effect on freedom of expression and the diversity of legal content available to consumers. The case study by Dan Isaksson, referenced in the user's prompt, likely provides detailed examples of how this dynamic plays out and its detrimental effects on individuals and businesses within the adult sector. The core of the challenge lies in the disproportionate power held by a few large payment processors, whose policies can dictate market access for entire categories of legal commerce based on their own risk appetites or moral stances, rather than solely on legal mandates.

The mechanisms through which "definitional creep" operates are often tied to the risk management practices of financial institutions. Adult content is frequently classified as a **"high-risk" merchant category (MCC 5764)**, subjecting businesses in this sector to stricter scrutiny, higher fees, and more stringent contractual terms from payment processors . This classification is often based on factors like higher chargeback rates

or the potential for fraudulent activity, but it can also be influenced by the perceived reputational risk associated with adult material. Payment processors, in their efforts to mitigate these risks, may adopt overly broad definitions of what constitutes unacceptable content, leading to the suppression of legal material that falls outside their subjective comfort zones. This creates an environment where creators and platforms must constantly navigate a shifting landscape of unwritten rules, fearing deplatforming or loss of payment services if they inadvertently cross an ambiguous line. The lack of clear, consistent, and publicly accountable standards from these financial gatekeepers is a fundamental challenge for the adult industry, impacting livelihoods and limiting the diversity of sexual expression available online .

### 4.2. Potential for the Digital Euro to Mitigate Payment Processor Influence

The EU Digital Euro, as a publicly issued and governed central bank digital currency, **holds the potential to mitigate some aspects of payment processor influence**, particularly the "definitional creep" that affects legal adult content. By providing an alternative payment rail that is not directly controlled by private, profit-driven corporations like Visa and Mastercard, the digital euro could reduce the leverage these entities currently hold over platforms and content creators . If the digital euro offers robust privacy features, especially for offline or low-value transactions, it could allow users to make payments for sensitive but legal content with less fear of data tracking or discrimination based on the nature of their transactions . The Eurosystem's commitment not to use personal data for commercial purposes is a significant departure from the practices of many private payment providers . Furthermore, if the digital euro achieves widespread acceptance and is designed to be a cost-effective option for merchants, it could provide a viable alternative to traditional card networks, potentially empowering platforms to resist pressure to censor content based on processor policies.

However, the extent of this mitigation is not absolute. The digital euro will still rely on **Payment Service Providers (PSPs) for distribution, user onboarding, and interface management** . These PSPs will be subject to EU regulations, including stringent Anti-Money Laundering (AML) and Counter-Terrorism Financing (CFT) requirements, which necessitate customer due diligence and transaction monitoring . If PSPs, in fulfilling these obligations or due to their own risk assessments, adopt cautious stances towards certain merchant categories (like adult content), they could still act as gatekeepers and potentially replicate some of the restrictive practices seen with current payment processors. The success of the digital euro in truly mitigating payment processor

influence will therefore depend on the **specific regulatory framework governing PSPs' conduct**, the clarity of rules regarding acceptable content (which should be based on law, not private corporate policy), and the level of oversight to ensure fair and non-discriminatory access to the digital euro payment system. While it offers a promising alternative, it may not entirely eliminate the influence of intermediaries or the broader societal and regulatory pressures that shape the online environment for adult content.

### 4.3. Uncertainties and Limitations of the Digital Euro in Addressing These Issues

Despite its potential, the EU Digital Euro faces **significant uncertainties and limitations in fully addressing the issues of payment processor influence and "definitional creep"** over adult content. A primary limitation stems from the continued role of **Payment Service Providers (PSPs)** in the digital euro ecosystem . PSPs will be responsible for user onboarding, KYC/AML checks, and providing the user interface for digital euro transactions. While the Eurosystem aims to minimize its own access to personal transaction data, PSPs will necessarily have visibility and will be bound by EU regulations, including AML/CFT directives . This means that if PSPs perceive adult content providers as high-risk or if they face pressure (regulatory or reputational) to restrict services to this sector, they might still deny access or apply stringent scrutiny, potentially perpetuating financial exclusion. The "definitional creep" could simply shift from being dictated by global card networks to being influenced by the risk appetites and interpretations of individual PSPs operating within the digital euro framework, unless specific safeguards are implemented.

Furthermore, the **broader EU regulatory landscape, particularly the Digital Services Act (DSA)**, will continue to apply to platforms hosting adult content . The DSA imposes obligations on platforms regarding illegal content, protection of minors, and transparency, which could indirectly affect payment processing. If platforms are required to implement more stringent content moderation or age verification, this could intersect with payment data and user identification, regardless of the payment instrument used. The digital euro itself will not override these platform-level obligations. Additionally, the **final design of the digital euro's privacy features, especially the transaction limits for offline and pseudonymous payments, will be crucial** . If these limits are too low, they may not be practical for many transactions within the adult industry. The legal status of various adult activities also varies across EU member states, adding another layer of complexity. Ultimately, while the digital euro offers a potential pathway to greater payment privacy and reduced reliance on a few dominant private processors, it is not a panacea and will operate within a complex web

of existing financial regulations, content laws, and the operational decisions of intermediaries.

### 4.4. Role of Payment Service Providers (PSPs) in the Digital Euro Ecosystem

**Payment Service Providers (PSPs) will play a crucial and multifaceted role in the digital euro ecosystem**, acting as the primary interface between end-users and the Eurosystem. Their responsibilities are expected to include **user onboarding, which involves Know Your Customer (KYC) and Anti-Money Laundering (AML) checks**, managing digital euro accounts, providing payment initiation services, and offering user support . While the Eurosystem will oversee the settlement infrastructure and ensure the integrity of the digital euro as a currency, PSPs will be the entities that individuals and businesses interact with on a daily basis to access and use the digital euro. This distribution model means that PSPs will have access to user data to the extent necessary to fulfill their regulatory obligations and provide their services. The European Commission's proposal envisages that all PSPs approved under PSD2 may provide digital euro distribution services, and specific obligations are placed on account servicing payment service providers (ASPSPs) to enable easy funding and defunding between digital euro accounts and traditional bank accounts or cash .

The involvement of PSPs introduces both opportunities and challenges concerning sensitive payments. On one hand, a diverse range of PSPs could foster competition and innovation in user-facing services, potentially leading to more tailored solutions. On the other hand, PSPs will remain subject to EU laws, including AML/CFT regulations, which require them to monitor transactions and report suspicious activity . This means that **PSPs will be gatekeepers to the digital euro system**. If PSPs adopt overly restrictive interpretations of their AML/CFT duties or apply their own terms of service that discriminate against legal but sensitive businesses (such as those in the adult industry), the privacy benefits of the digital euro at the Eurosystem level could be undermined at the point of user access. The European Banking Federation (EBF) has noted that commercial banks must have access to customer data to perform regulatory checks, and there should be the same rules for all digital payments, including CBDCs . Therefore, the regulatory framework governing PSPs' conduct, their compensation models, and the oversight mechanisms to ensure fair access will be critical in determining whether the digital euro can provide a genuinely inclusive and less censorious payment option.

### 4.5. The Digital Euro's Geopolitical Ambitions and Reducing Foreign Dependence

A significant driver behind the EU Digital Euro project is the **geopolitical ambition to enhance Europe's strategic autonomy and reduce its dependence on foreign payment systems and technologies** . Currently, a substantial portion of digital payments in the euro area, particularly card transactions, are processed by a few dominant international card schemes (ICS) and e-payment solutions, many of which are non-European . This reliance on foreign providers raises concerns about European sovereignty, the ability to set its own standards, and potential vulnerabilities in critical financial infrastructure. The digital euro is envisioned as a **pan-European payment solution operating under European governance**, which could strengthen the international role of the euro and offer a resilient alternative to foreign payment providers . By providing a public digital currency, the EU aims to ensure that central bank money remains an anchor for the payment system in an increasingly digitalized economy, preserving public trust and European control over its monetary landscape .

This ambition to reduce foreign dependence has implications for sensitive payments, including those for adult content. If the digital euro successfully provides a viable, cost-effective, and privacy-enhanced European alternative to current payment rails, it could lessen the influence of non-European payment processors whose policies often drive "definitional creep" and financial censorship . A European public payment infrastructure, governed by EU laws and values, might offer a more stable and predictable environment for legal businesses, including those in sensitive sectors. The ECB suggests that the introduction of the digital euro could give merchants a better negotiating position versus international card schemes and payment processors, potentially leading to lower costs and reduced reliance on their terms of service . While PSPs will still be involved, the underlying currency and core infrastructure would be European, potentially fostering a payment ecosystem more aligned with European public policy objectives, including the protection of fundamental rights and the promotion of a competitive digital single market. This strategic dimension adds another layer to the potential impact of the digital euro beyond its technical and privacy features.