



Report

Global Age-Verification Laws: 2025 Snapshot

Key Regulations and Their Business Impact

Copyright © Shufti Ltd. All Rights Reserved.



VÉRIFICATION
D'ÂGE KJM



PCI DSS



iBeta Niveau 1



ISO 27001: 2013



CE+



QG GDPR



SOC2



GDPR



CCPA



Table of Contents

Evolving Requirement of Age Verification	01
How Regulation Is Transforming Age Verification Across Digital Ecosystems	01
Industries Impacted by Emerging Age-Verification Laws	02
Jurisdictional Summaries and Compliance Sources	03
4.1 United States (selected state laws now in force or operating)	03
4.1.1 Texas (House Bill 1181- From the 88th Legislature)	03
4.1.2 Louisiana (Act 440; R.S. 9:2800.29)	03
4.1.3 Utah (S.B. 287 — Online Pornography Viewing Age Requirements, 2023)	03
4.1.4 Mississippi (SB 2346 — 2023)	04
4.1.5 Virginia (SB 1515 — 2023; Va. Code § 8.01-40.5)	04
4.1.6 Florida (HB 3 — 2024; Fla. Stat. §§ 501.1736–501.1738)	04
4.1.7 North Carolina (HB 8 — PAVE Act)	05
4.2 United Kingdom	05
4.2.1 Online Safety Act 2023 (Part 5; Ofcom Codes)	05
4.2.2 Retail Alcohol (Licensing Act Mandatory Conditions)	05
4.3 European Union and Key Member States	06
4.3.1 EU Commission Age-Verification Blueprint (2025)	06
4.3.2 France (ARCOM Référentiel)	06

4.3.3 Germany (JMSTV; KJM Criteria)	07
4.3.4 Ireland (Online Safety Code for VSPs)	07
4.3.5 Italy (AGCOM, 2025)	07
4.3.6 Spain (Policy Direction On Social Media Minimum Age)	07
4.4 Asia-Pacific	08
4.4.1 Australia (Social-Media Minimum Age; eSafety Expectations)	08
4.4.2 Singapore (IMDA Codes — Social Media Services & App Distribution Services)	08
4.4.3 Japan (Act No. 79 of 2008)	08
4.4.4 South Korea (Youth Protection Act; ICN Frameworks)	09
4.5 Middle East & Africa	09
4.5.1 United Arab Emirates (TDRA — Internet Access Management Policy)	09
4.5.2 Saudi Arabia (GAMR/GCAM — Classification & Licensing)	09
4.5.3 South Africa (Films and Publications Act; 2019 Amendments & 2022 Regulations)	10
4.6 Latin America	10
4.6.1 Brazil (Classificação Indicativa & New Digital Child-protection Rules)	10
Implementation Notes for Businesses	11

Evolving Requirement of Age Verification

A new compliance dilemma has taken center stage for digital and even certain brick and mortar businesses: how to prove a user's age without causing drop-offs due to friction. Age verification has shifted from a voluntary practice to a statutory duty in many jurisdictions.

Across industries, friction-heavy age verification methods, such as uploading documents, performing facial scans, or conducting manual checks, are driving customer drop-off, extending onboarding time, and depressing conversion rates. The result is a growing tension between compliance and commercial viability: protect minors effectively while preserving a seamless user experience.

This pressure has turned age assurance into a strategic priority for platforms, retailers, and content providers alike. Regulators are demanding stronger evidence that minors cannot access restricted content or services, while users increasingly expect seamless, privacy-first digital journeys.

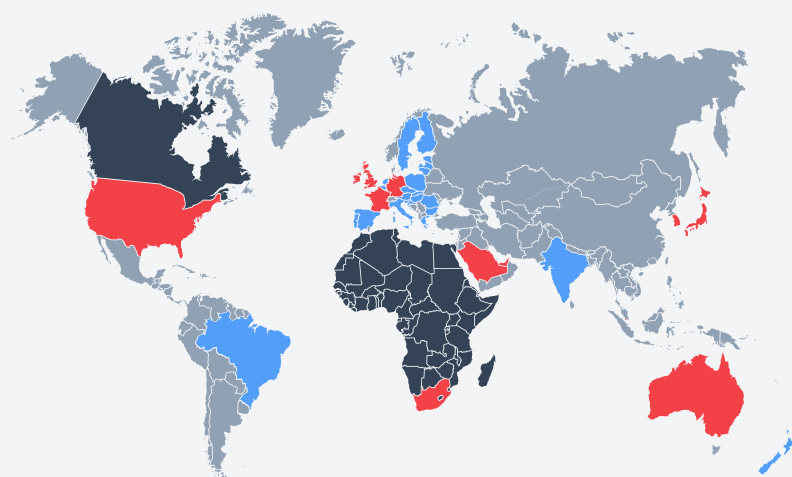
The businesses that succeed will be those that implement low-friction, privacy-preserving verification systems that meet statutory standards while safeguarding trust and conversion.

Global Compliance Choropleth

Age-verification laws, which are active, pending, or in consultation in certain regions.

Key:

- Active Laws
- Laws in Draft/Consultation
- No Current Regulation



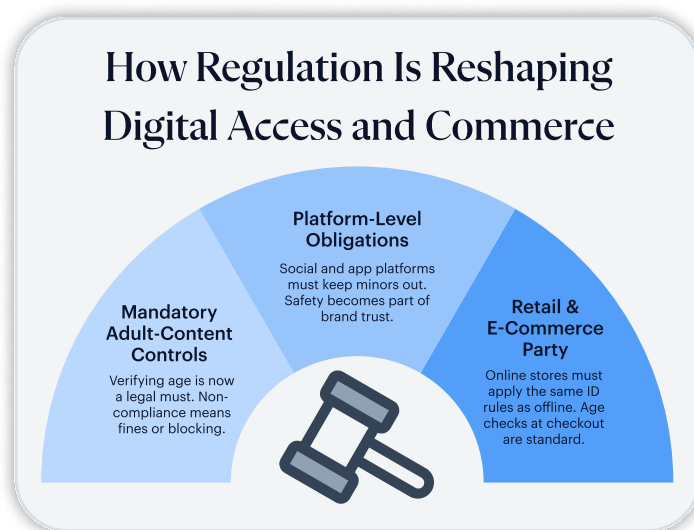
How Regulation Is Transforming Age Verification Across Digital Ecosystems

1. Online adult-content access controls have become legally mandated across multiple jurisdictions, with clear expectations for robust, privacy-respecting verification.

2. Obligations are expanding beyond adult content into platform-level controls governing social media account eligibility and app store distribution.
3. Long-standing retail age checks, for alcohol, gambling, or tobacco, are now being mirrored online, setting the baseline for digital compliance.

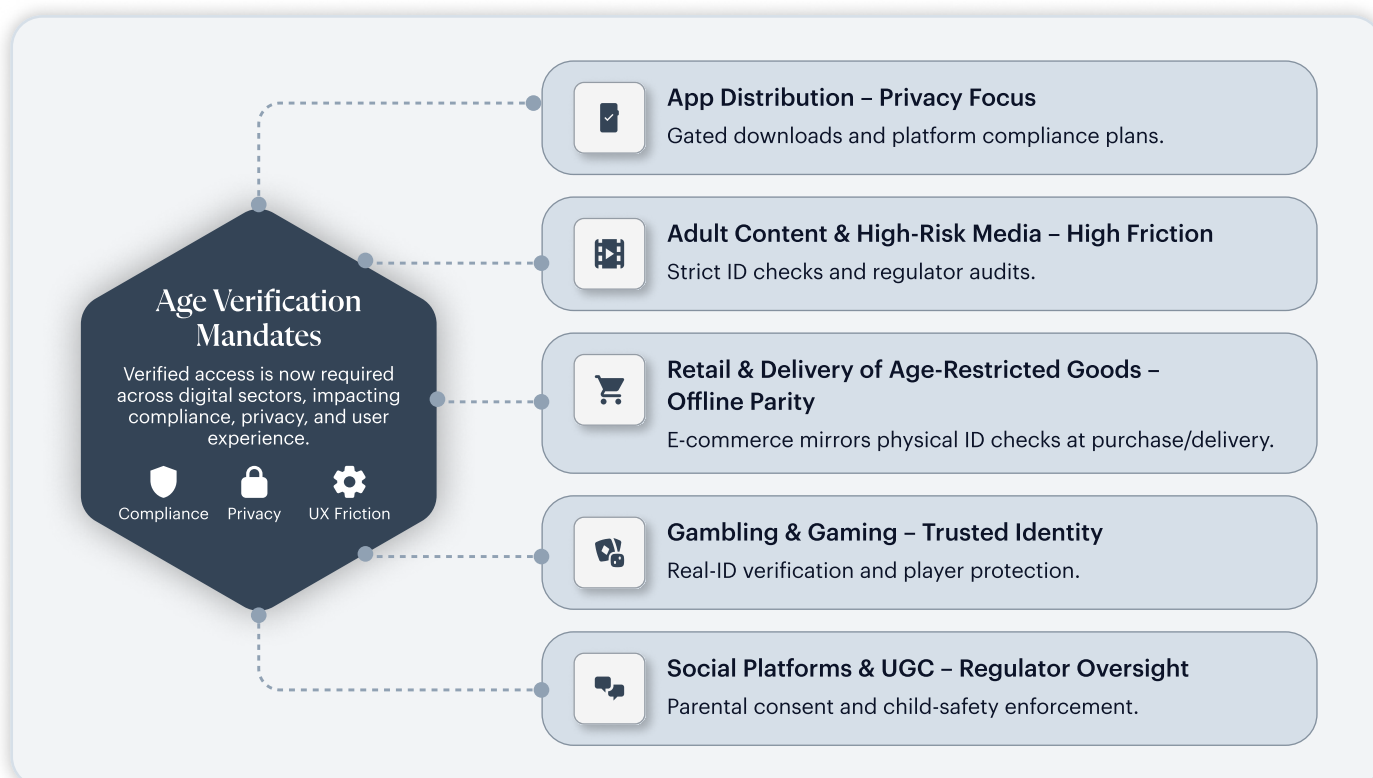
Businesses now need to develop adaptive age-verification frameworks that can range from simple, low-friction checks to more rigorous document or credential-based verifications, in line with legal requirements.

They must do this while ensuring that personal data is not retained, complying with jurisdiction-specific regulations, and maintaining clear audit records.



Industries Impacted by Emerging Age-Verification Laws

The regulatory net now spans a wide spectrum of digital and commercial sectors. Key industries in scope include, but are not limited to:



Jurisdictional Summaries and Compliance Sources

United States (selected state laws now in force or operating)

◉ Texas (House Bill 1181- From the 88th Legislature)

Scope: This applies to commercial websites that feature more than one-third of their content as 'sexual material harmful to minors.' However, exemptions are in place for legitimate news and public interest content, and protections are provided for ISPs, search engines, and cloud providers if they aren't responsible for the content.

Methods: Mandates the implementation of 'reasonable age verification' through digital identification or commercial age verification methods that utilize government-issued IDs or transaction data checks, while ensuring strict non-retention of any identifying information.

Sectors: Online publishers of adult content and platforms that host such materials.

Source: <https://capitol.texas.gov/tlodocs/88R/billtext/pdf/HB01181F.pdf>

◉ Louisiana (Act 440; R.S. 9:2800.29)

Scope: This applies to sites where a significant portion (more than 33⅓%) is considered materially harmful to minors. Additionally, there are exemptions and protections reminiscent of Texas law.

Methods: Permits the use of digitized IDs (such as LA Wallet) or commercial age verification services that rely on government-issued IDs or transactional data, along with a clear mandate for non-retention of information.

Sectors: Publishers and platforms providing online adult content in Louisiana.

Source: <https://legis.la.gov/legis/ViewDocument.aspx?d=1289498>

◉ Utah (S.B. 287 — Online Pornography Viewing Age Requirements, 2023)

Scope: This applies to websites where over one-third (33⅓%) of the total content is deemed harmful to minors. However, there are exemptions for legitimate news sources and intermediaries.

Methods: Permits the use of digitized IDs, allows third-party comparisons of autonomous vehicle data against databases, and enables checks of transactional data; additionally, it mandates non-retention and provides a private right of action.

Sectors: Online adult-content publishers and platforms over the threshold.

Source: <https://le.utah.gov/~2023/bills/sbillenr/SB0287.pdf>

● Mississippi (SB 2346 — 2023)

Scope: This applies to websites where over one-third of the content is deemed harmful to minors; it includes provisions for exemptions and protections for intermediaries.

Methods: The process requires a reasonable level of authentication through digitized identification or commercial verification, such as a government ID or transactional data. Furthermore, there are provisions for non-retention and civil remedies.

Sectors: Online adult-content publishers and platforms over the threshold.

Source: <https://law.justia.com/codes/mississippi/title-11/chapter-77/section-11-77-5/>

● Virginia (SB 1515 — 2023; Va. Code § 8.01-40.5)

Scope: This applies to websites where over one-third of the total content is considered harmful to minors. In such cases, interactive computer service providers and users are not held liable under this section.

Methods: Take appropriate measures to confirm that individuals are 18 years or older through commercial databases or other reliable methods for verifying age and identity. Failure to comply may result in civil liability.

Sectors: Online adult-content publishers and platforms over the threshold.

Source: <https://law.lis.virginia.gov/vacode/title8.01/chapter3/section8.01-40.5/>

● Florida (HB 3 — 2024; Fla. Stat. §§ 501.1736–501.1738)

Scope: To safeguard minors, restrict access to adult content where over 33.3% of the material may be harmful. Regarding social media, prohibit accounts for those under 14, require verified parental permission for users aged 14 to 15, and ensure the termination of underage accounts while deleting personal data unless legally required to retain it.

Methods: For adult content, anonymous adult verification must be conducted by a third-party provider located in the United States that does not retain any records. Standard adult-verification procedures used by government entities and businesses apply, and compliance is enforced under the Florida Deceptive and Unfair Trade Practices Act (FDUTPA).

For social media, multiple adult-verification mechanisms are permissible, and parental or guardian consent must be formally verified.

Sectors: Adult-content websites/apps and social-media platforms offering accounts to Florida users.

Source: <https://www.flsenate.gov/laws/statutes/2024/501.1736>

◉ North Carolina (HB 8 — PAVE Act)

Scope: This applies to sites where over 33⅓% of the content is considered harmful to minors; it includes exemptions and protections for intermediaries.

Methods: Age verification should be conducted through commercial databases or other reasonable methods for confirming age and identity. Additionally, it's important to implement non-retention practices and uphold a private right of action.

Sectors: Online adult-content publishers and platforms over the threshold.

Source: ncleg.gov/EnactedLegislation/SessionLaws/HTML/2023-2024/SL2023-132.html

United Kingdom

◉ Online Safety Act 2023 (Part 5; Ofcom Codes)

Scope: Part 5 emphasizes that services producing their own pornographic content must take steps to ensure children do not inadvertently come across it. Additionally, user-to-user and search services deemed higher risk have obligations regarding child safety, which may include verifying users' ages.

Methods: A technology-neutral standard is needed for 'highly effective' age assurance methods. Potential options include facial age estimation, photo-ID verification, digital/eID solutions, and cross-checks with trusted data sources. It's essential to implement strong privacy controls throughout the process.

Sectors: Adult-content services and higher-risk platforms operating in the UK.

Source: <https://www.legislation.gov.uk/ukpga/2023/50>

◉ Retail Alcohol (Licensing Act Mandatory Conditions)

Scope: Both on-premise and remote or online alcohol sales and deliveries must adhere to an age-verification policy as stipulated by the Licensing Act 2003 and the related statutory guidance.

Methods: Challenge 21/25 mandates that acceptable forms of photo ID, such as a passport, photocard driving license, or PASS card, must be presented prior to any sale, supply, or delivery. This policy also emphasizes the importance of staff training and the logging of any refusals.

Sectors: Retailers, off-licences, supermarkets, hospitality venues, and delivery/remote-sale operators.

Source: <https://www.legislation.gov.uk/ukdsi/2014/978011116906>

European Union and Key Member States

● EU Commission Age-Verification Blueprint (2025)

Scope: A reference model (not legally binding) that outlines the responsibilities for protecting minors under the DSA and ensuring compatibility with the EU Digital Identity Wallet (EUDI).

Methods: Disclosing age attributes selectively with wallet-compatible, privacy-focused components; ensuring minimal exposure of personal data.

Sectors: Any service that must enforce age gates under EU/Member-State rules.

Source: <https://www.biometricupdate.com/202510/eu-updates-age-verification-blueprint-app-amid-debate-on-social-media-restrictions>

● France (ARCOM Référentiel)

Scope: Law No. 2024-449, enacted on May 21, 2024, aims to secure and regulate the digital space by requiring that pornographic services available in France implement measures to prevent minors from accessing this content. Oversight of these regulations will be provided by the audiovisual and digital regulator, ARCOM.

Methods: ARCOM sets forth essential technical standards for age-verification systems through its framework, highlighting the importance of privacy-preserving measures and independent-intermediary verification, often referred to as “double-anonymity.” Websites that do not comply with these standards could face a range of penalties, including formal notices, fines, potential removal from search engine listings within 48 hours, or blocking orders sanctioned by administrative courts.

Sectors: Online pornographic publishers and video-sharing platforms accessible in France.

Source: https://www.legifrance.gouv.fr/download/pdf?id=1kWAYP9AsPTUa6nbDcb3Sq3PzXyH1U2x_naRfEud_Wg=

🕒 Germany (JMSTV; KJM Criteria)

Scope: Content deemed harmful to minors should be accessible only within a 'closed user group' designated for adults. KJM assesses AVS concepts accordingly.

Methods: Reliable age verification methods (ID/eID/video identification) combined with strong authentication have received positive evaluations from KJM.

Sectors: Adult content and youth-restricted media offered online in Germany.

Source: <https://www.kjm-online.de/themen/technischer-jugendmedienschutz/unzulaessige-inhalte/>

🕒 Ireland (Online Safety Code for VSPs)

Scope: Designated VSPs are required to implement measures that safeguard users, such as age verification, to shield them from exposure to pornography or excessive violence.

Methods: A balanced approach to age-assurance and verification at the platform level, coupled with oversight enforcement and significant penalties for violations.

Sectors: UGC/video-sharing platforms designated under the Code.

Source: <https://www.gov.ie/en/department-of-culture-communications-and-sport/publications/online-safety-and-media-regulation-act-2022/>

🕒 Italy (AGCOM, 2025)

Scope: Starting from November 12, 2025, services providing access to pornographic content in Italy will be required to verify that their users are adults.

Methods: Certified AV schemes that prioritize privacy from the ground up and align with EU standards may face fines and possible restrictions.

Sectors: Online adult-content sites and platforms accessible in Italy.

Source: <https://www.agcom.it/comunicazione/comunicati-stampa/comunicato-stampa-del-07-ottobre-2024>

🕒 Spain (Policy Direction On Social Media Minimum Age)

Scope: A national framework is being established to raise the minimum age for social media use and implement effective audiovisual and child-safety measures. Additional details will be released as the measures are progressively implemented.

Methods: Mechanisms that are anticipated to uphold privacy standards while being compatible with EU regulations (such as selective disclosure that aligns with EUDI) are expected to be in place.

Sectors: Social-media platforms operating in Spain.

Source: <https://www.surinenglish.com/spain/the-government-approves-the-law-that-raises-20250326064806-nt.html>

Asia–Pacific

● Australia (Social-Media Minimum Age; eSafety Expectations)

Scope: Social media platforms designated for this purpose are required to block accounts for users under 16 starting on December 10, 2025. The eSafety office will oversee and enforce this policy.

Methods: A technology-neutral and demonstrably effective approach to age assurance is in alignment with BOSE/eSafety standards, incorporating age estimation, identity verification, digital ID wallets, and trusted data checks.

Sectors: Social-media platforms and high-risk services within eSafety’s remit.

Source: <https://www.esafety.gov.au/about-us/industry-regulation/social-media-age-restrictions/campaign>

● Singapore (IMDA Codes — Social Media Services & App Distribution Services)

Scope: This applies to specific social media platforms as of July 18, 2023, and will take effect for major app stores on March 31, 2025. The responsibilities include measures to prevent children from accessing apps that are not suitable for their age.

Methods: Age assurance and content gating should align with platform-level ratings and risk assessments. App stores are required to submit implementation plans and adhere to the PDPA's limits on data minimization and retention.

Sectors: Social platforms, app marketplaces/app stores, and games distributed via those marketplaces.

Source: <https://www.imda.gov.sg/regulations-and-licensing-listing/content>

● Japan (Act No. 79 of 2008)

Scope: A national framework has been established to safeguard users under 18 by placing responsibilities on internet service providers, mobile carriers, and other operators. The government's Basic Plans outline specific measures to implement these protections effectively.

Methods: Prioritize the responsibilities of filtering and providers, ensuring that sites suitable for youth are properly accredited, and establish clear reporting mechanisms.

Device and operating system manufacturers should play a key role in facilitating effective filtering.

Sectors: Broad online services and access providers engaged in youth protection.

Source: <https://www.japaneselawtranslation.go.jp/en/laws/view/1712>

South Korea (Youth Protection Act; ICN Frameworks)

Scope: Businesses that distribute or facilitate access to 'media harmful to juveniles' have a responsibility to ensure that minors cannot easily access such content. This obligation applies to both service providers and network providers alike.

Methods: Established methods for verifying age and identity, such as mobile phone authentication, electronic PINs, and certified credentials, along with filtering, labeling, and access controls, play a crucial role in ensuring security.

Sectors: Online media distributors, platforms hosting harmful material, and network providers.

Source: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=38401&lang=ENG

Middle East & Africa

United Arab Emirates (TDRA — Internet Access Management Policy)

Scope: A national, ISP-level regulation of restricted categories, such as pornography, that applies to all licensed Internet Service Providers.

Methods: ISPs implement network-wide blocking using TDRA-approved systems, with the TDRA responsible for defining and updating prohibited categories, as well as overseeing the relevant procedures.

Sectors: ISPs/telecom licensees and online media/services expected to avoid prohibited categories for UAE users.

Source: <https://tdra.gov.ae>

Saudi Arabia (GAMR/GCAM — Classification & Licensing)

Scope: Regulation and supervision of audiovisual and online media distribution, including video on demand (VOD), over-the-top (OTT) services, IPTV, streaming platforms, cinema, and video games.

Methods: Content classification and age-rating obligations should be accompanied by technical access controls as required. Platform policies must comply with these ratings.

Sectors: VOD/streaming and OTT platforms, IPTV services, cinemas, and online media/game distributors.

Source: <https://gmedia.gov.za/en/executive-regulations>

◉ South Africa (Films and Publications Act; 2019 Amendments & 2022 Regulations)

Scope: The amended Act now includes online distribution under the FPB's mandate. This means that online distributors are required to register and obtain permits, classify their content, and fulfill ongoing responsibilities.

Methods: Ensuring compliance through licensing and registration, as well as classification methods such as FPB ratings, Section 18C self-classification, or accepted foreign ratings, along with the display of age ratings and advisories.

Sectors: VOD/streaming platforms, online media services, and other commercial online distributors of films, games, and certain publications.

Source: <https://www.gov.za/documents/films-and-publications-act>

Latin America

◉ Brazil (Classificação Indicativa & New Digital Child-protection Rules)

Scope: The Classificação Indicativa system is applicable across the nation, covering broadcasts, cinema, television, video games, and on-demand or online content. With the measures set for 2025, this system will expand to include digital environments. Additionally, the Digital Statute for Children and Adolescents will outline specific responsibilities for platforms that are accessible to minors.

Methods: Services are required to clearly display mandatory age ratings and descriptors, and they must adhere to online distribution regulations. Providers should implement parental controls and settings that are suitable for different age groups. The 2025 ECA Digital anticipates the introduction of reliable age verification processes to restrict access to adult content.

Sectors: Streaming/VOD platforms and other online media distributors that make audiovisual content available in Brazil (including apps and online catalog services).

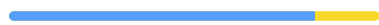
Source: <https://www.gov.br/mj/pt-br/assuntos/seus-direitos/classificacao>.

METHODS OF AGE VERIFICATION



Self-declared / Parental Consent

Simple form or checkbox; minimal data, easy user flow.



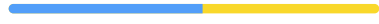
Privacy: High

Friction: Low



Digital ID (e.g., LA Wallet, eIDAS, EUDI)

Verified digital credentials; strong privacy, moderate user effort.



Privacy: High

Friction: Medium



AI-Based Age Estimation

Facial analysis or camera-based estimate; low effort, some data risk.



Privacy: Medium

Friction: Low



Credential-Based / Third-Party Verification

External verification services (transactional checks, trusted databases); rigorous but user-heavy.



Privacy: Medium

Friction: High



Government-Issued ID Upload

Passport/driver's license upload: higher security, more friction.



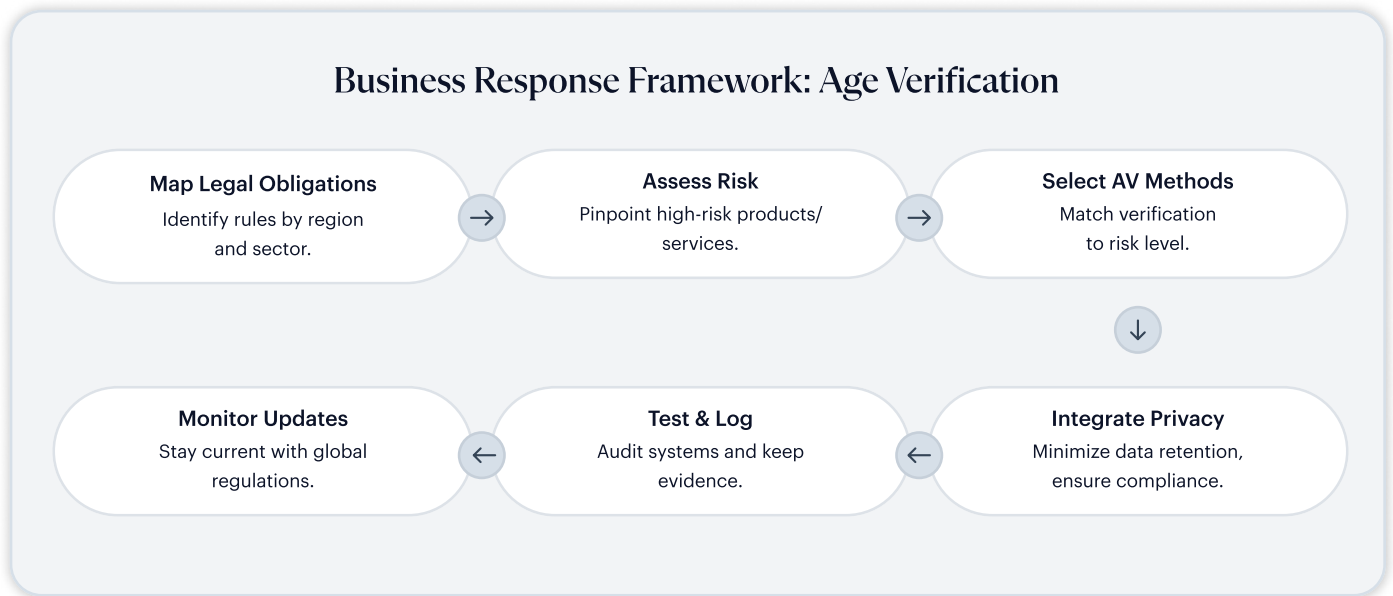
Privacy: Medium

Friction: High

Implementation of Age Verification-Guidelines for Businesses

- Align Product Areas with Legal Triggers:** Ensure each product area aligns with the relevant legal requirements, such as access to adult content, creating social media accounts, app distribution, gambling regulations, or the sale and delivery of age-restricted products.
- Provide Graduated Assurance:** Implement low-friction checks for low-risk engagements, and escalate to document or credential-based verification only when necessary due to statutory obligations or heightened risks.
- Set Up Jurisdiction Profiles:** Tailor the business jurisdiction profiles to incorporate non-retention stipulations, lists of accepted methods, notice language, and logging practices that comply with specific laws.

- Maintain Evidence of Compliance:** Keep thorough records of business policies, ensure vendor independence when needed, maintain decision logs, and preserve performance testing artifacts adequate for regulator review.





Privacy-First Age Verification

Shufti's adaptive age verification delivers fast, compliant, low-friction onboarding while accurately blocking minors, protecting privacy, reducing churn, and enabling confident scaling.

[Book a Free Demo](#)

