Meta Video Selfie Verification: GDPR Risks, Biometric Data and Privacy Concerns

Category: SMM Blog
November 8, 2026





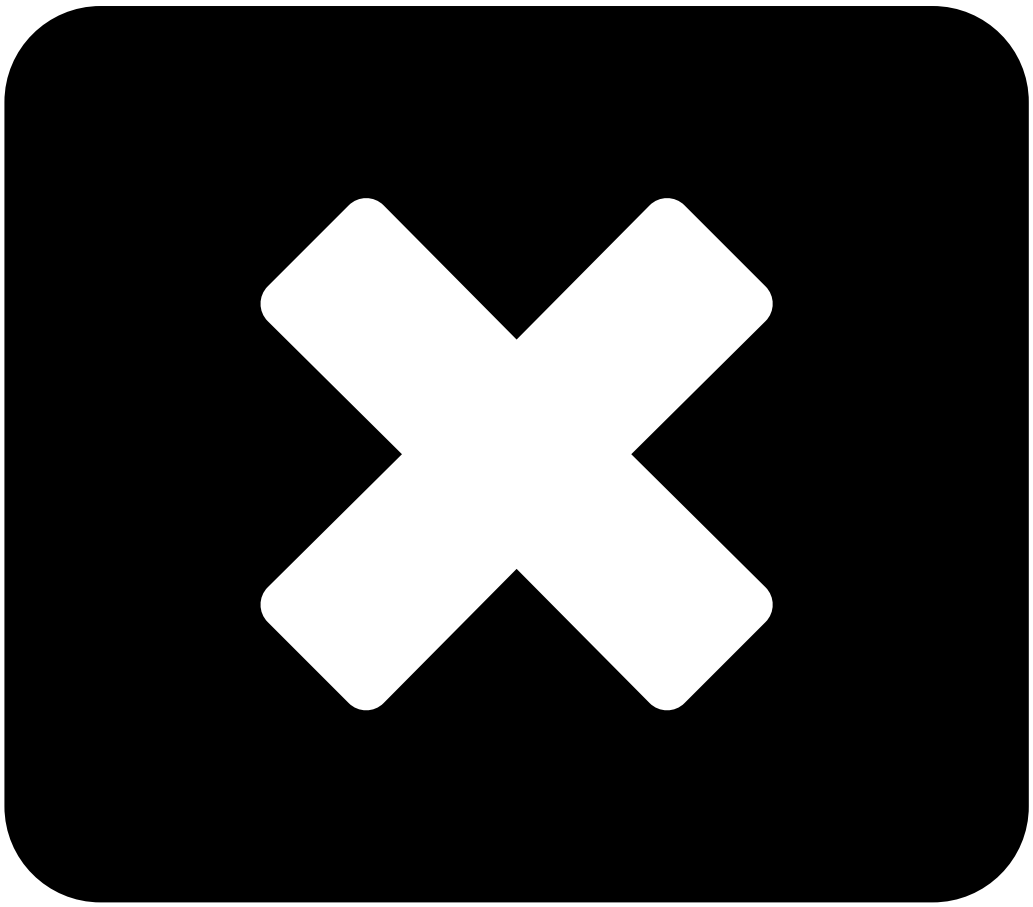
Hamburger Toggle Menu

[redacted]

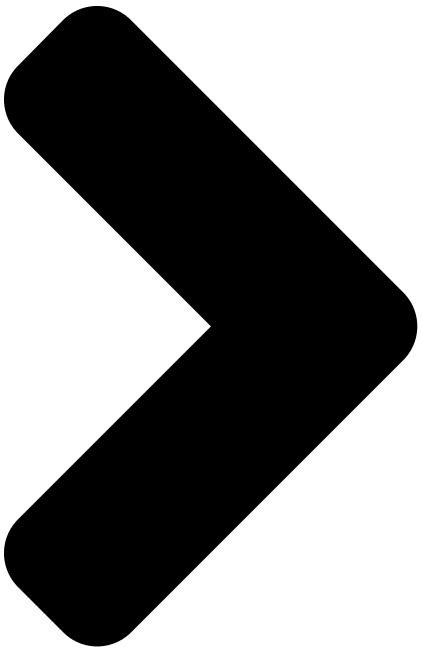
[redacted]

[redacted]

Free Quote

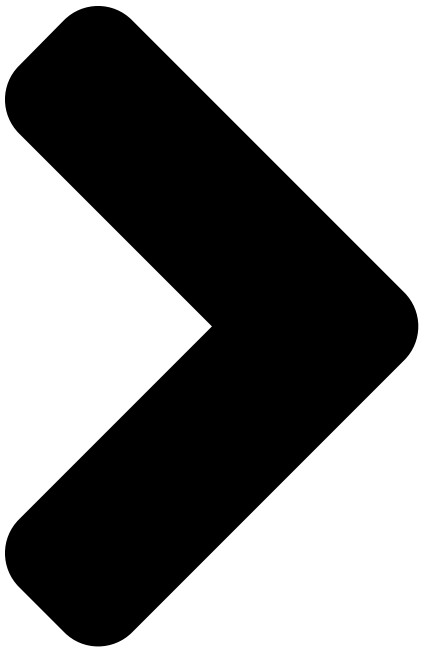


•

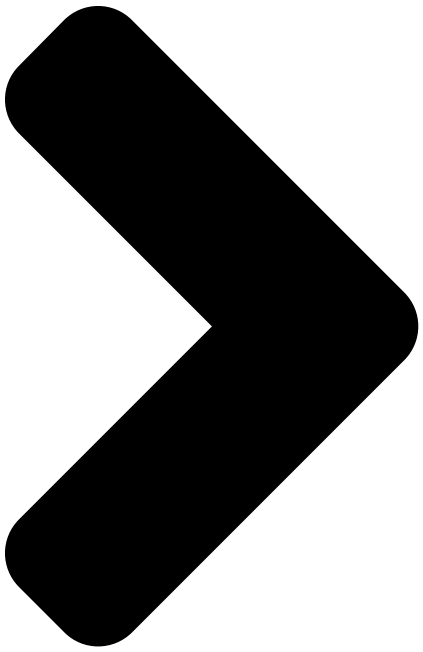


About us

-



Request for detailed website quote



Courses University TSI

-

Login Team TST Digital Solution

OUR PARTNERS











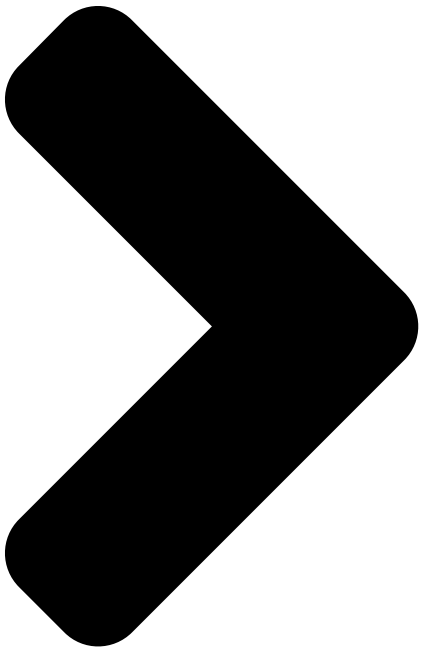


Trending Topic

Publicity

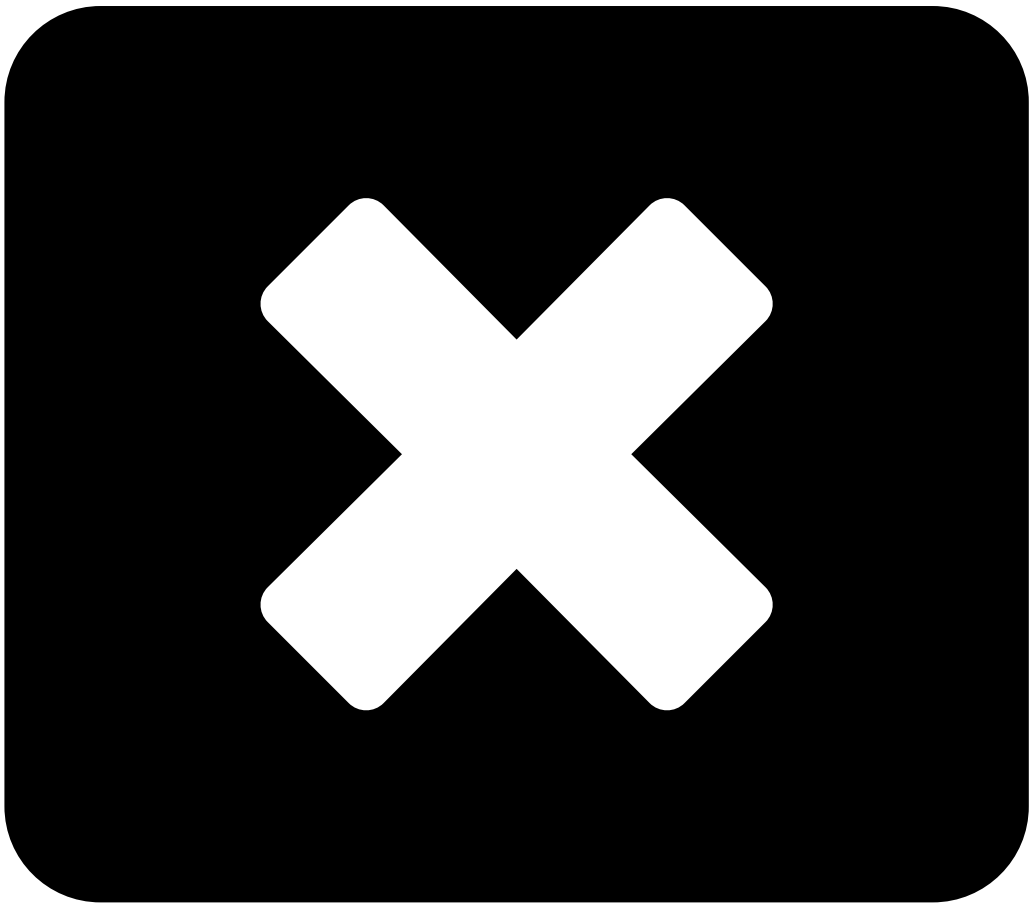
Reach out



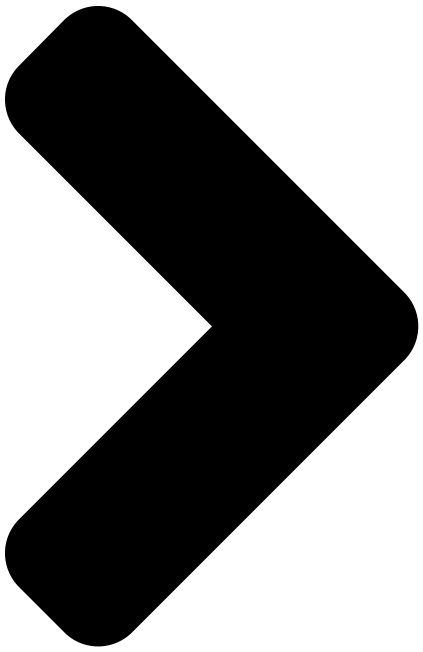


Some projects

Edit Template

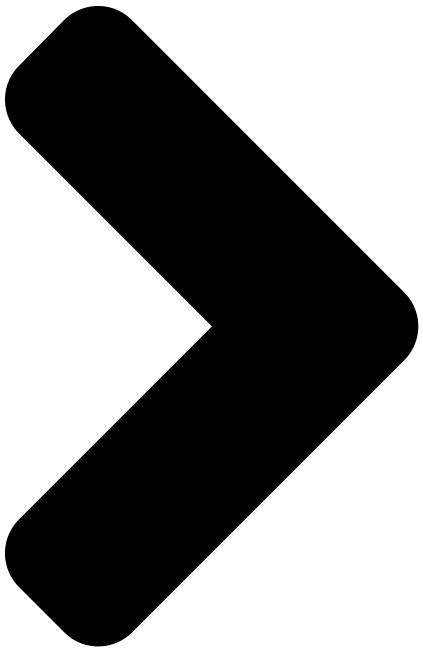


•

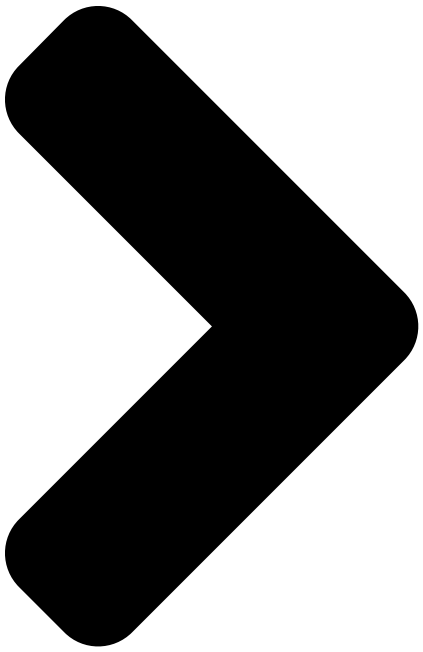


Services

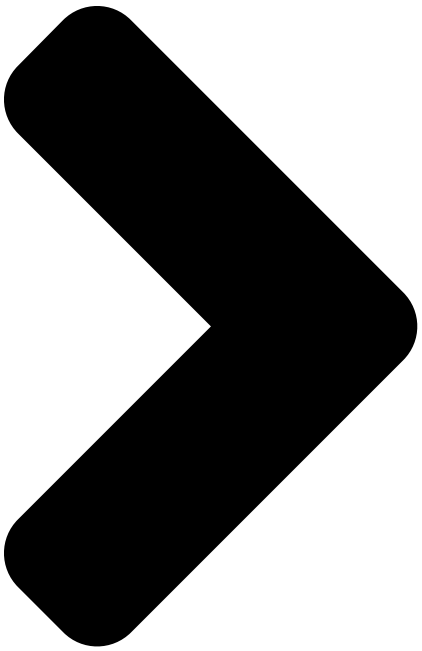
-



Web Design & Development

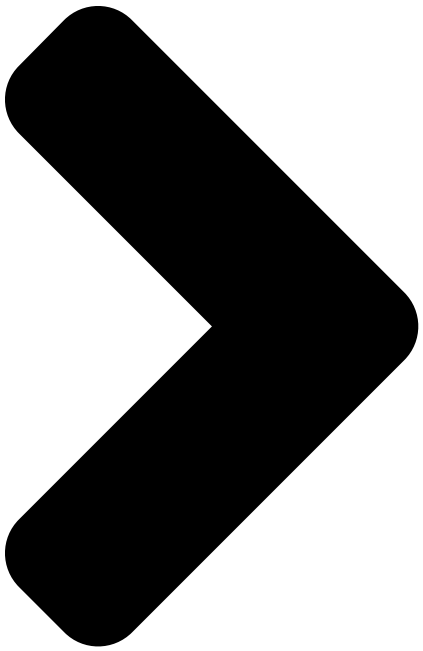


- Hosting
-

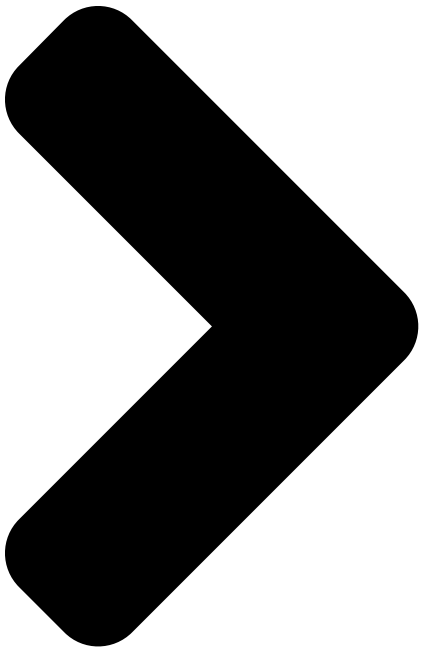


SEO/Ads/GMB/Speedup/Plugins/Technical

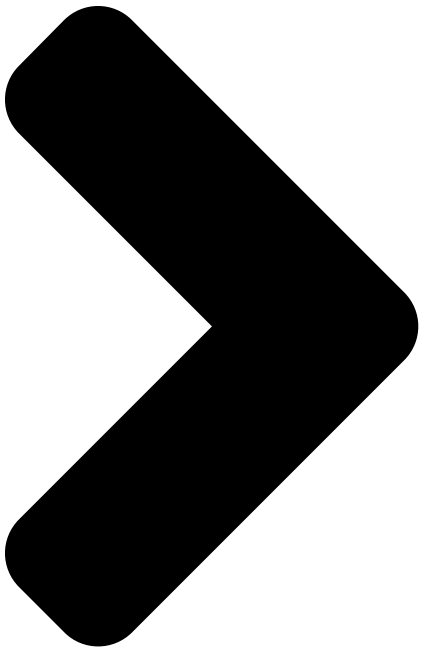
-



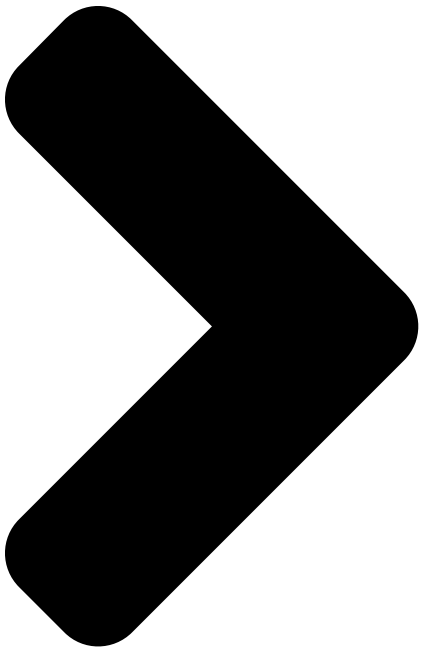
App Design & Development



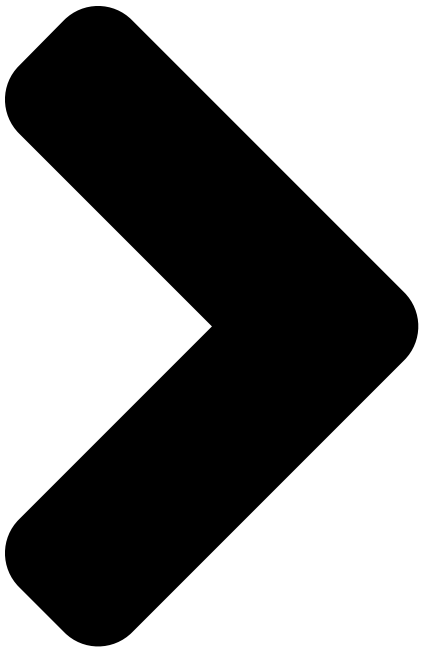
AI Agents



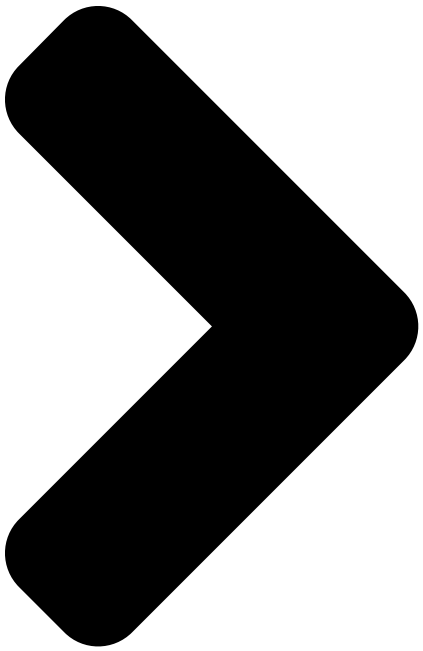
- e-Commerce
-



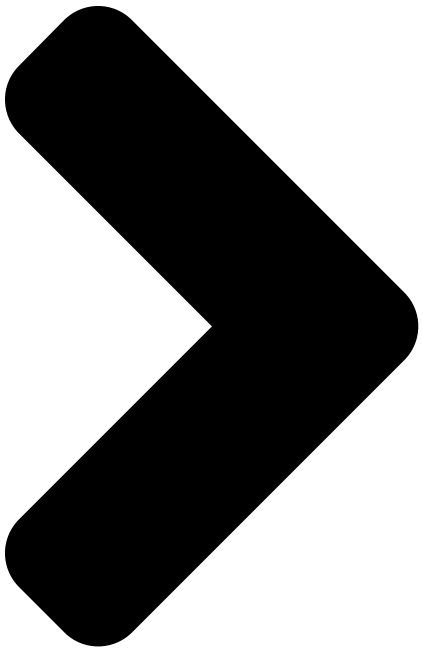
- Branding



- Social Media & Content Creation



- Graphic Design



- Copywriting & Translations

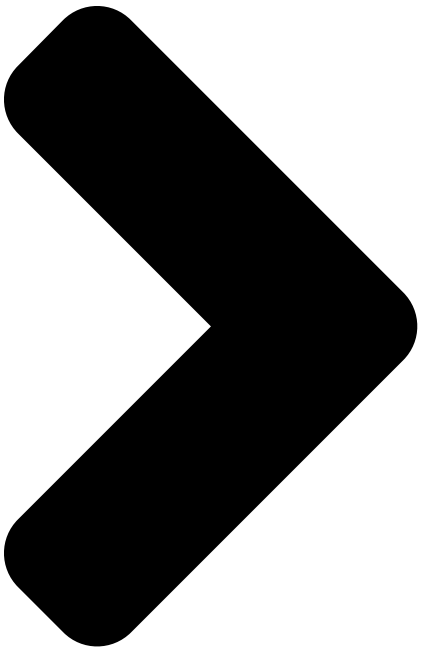


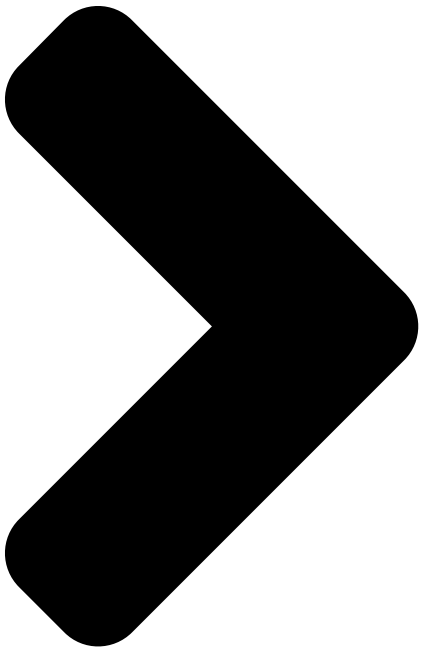
Photo- & Videography

Trending Topic

Publicity

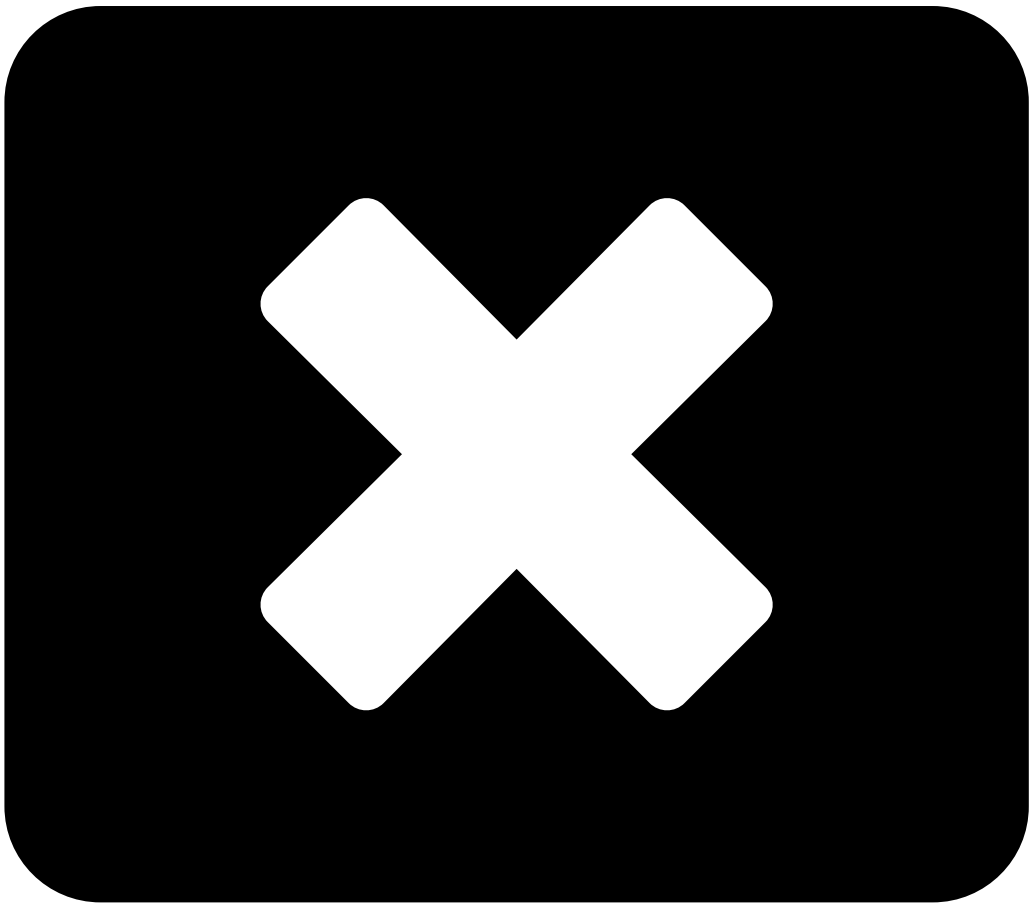
Calculate a quote
online yourself


Digital Solution

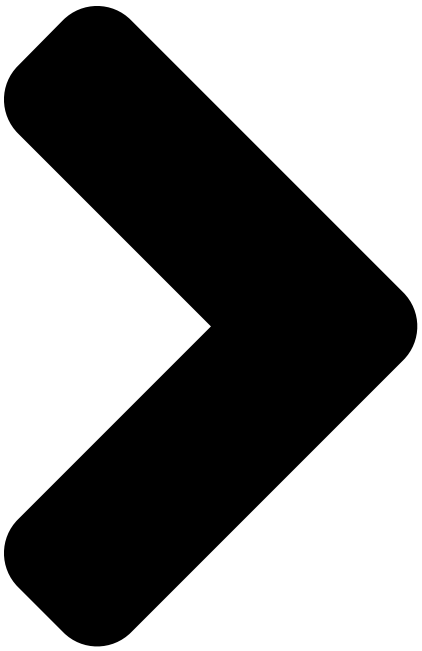


The way we work

Edit Template



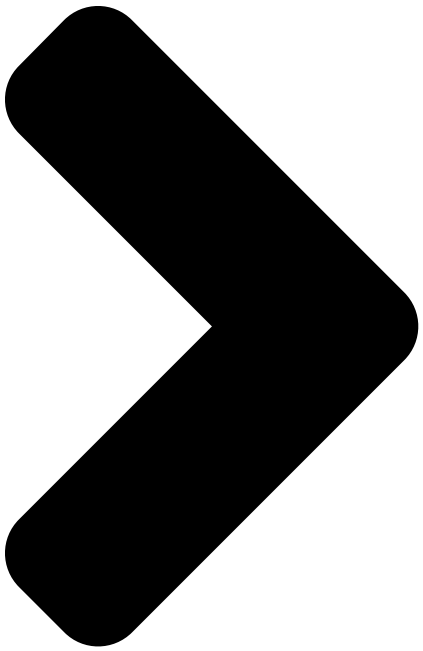
•



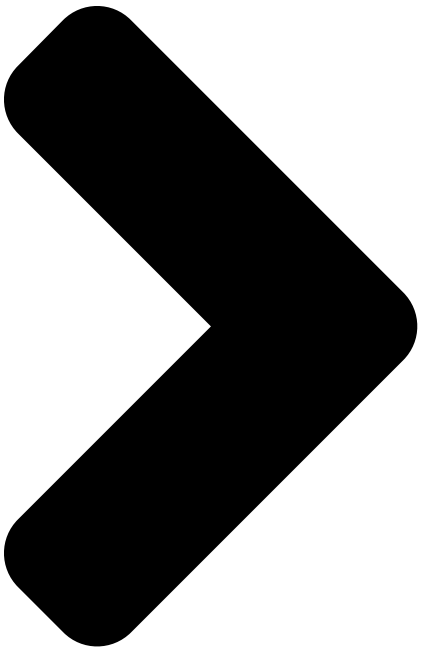
Realized projects

Calculators for your project costs

-



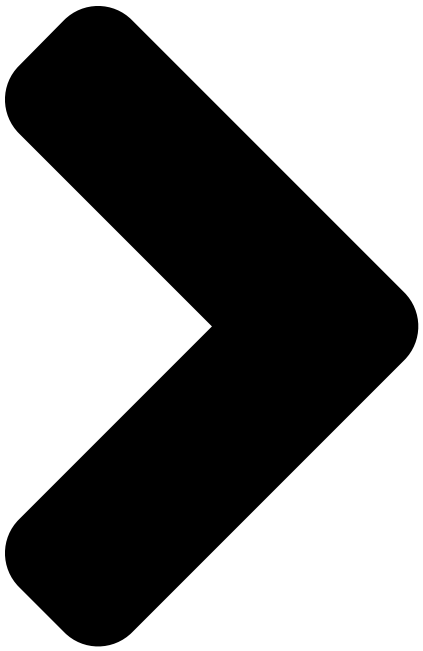
Request for detailed website quote



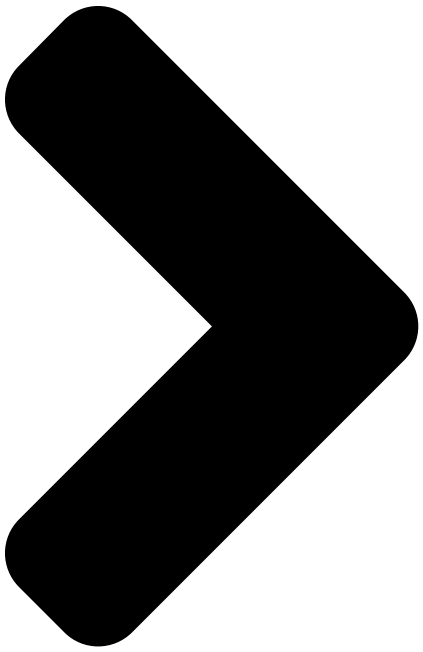
Overview of quote calculators

Useful information

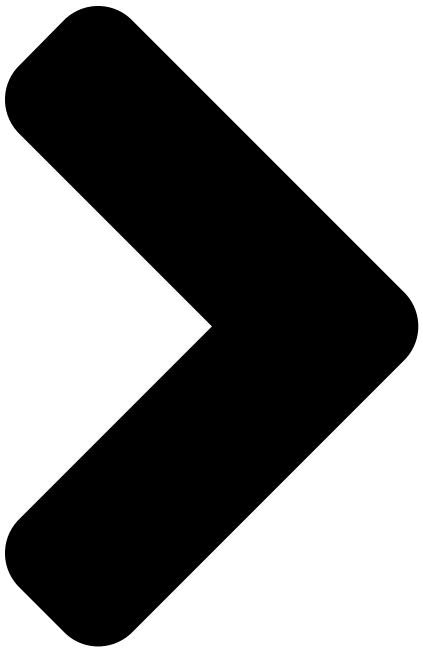
-



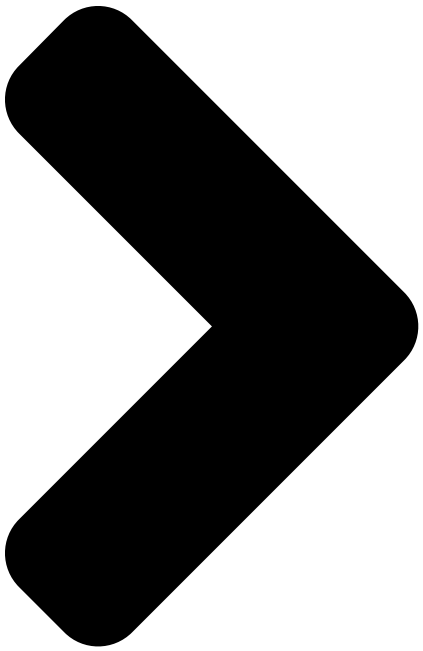
Jobs @ TSI Digital Solution



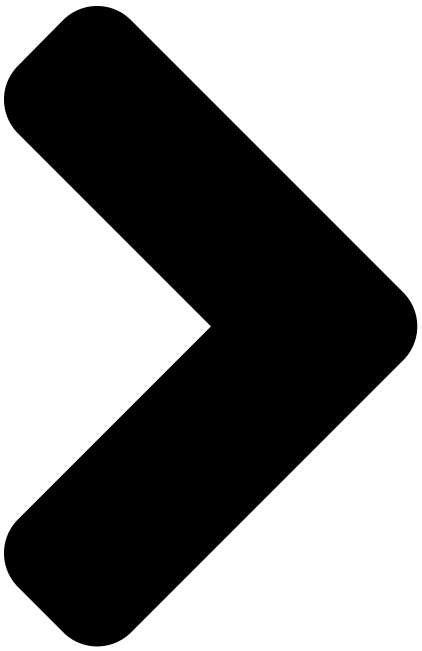
- Hosting at €75/year



TSI Free Tools



- WordPress plugin TSI Visitor Blocker



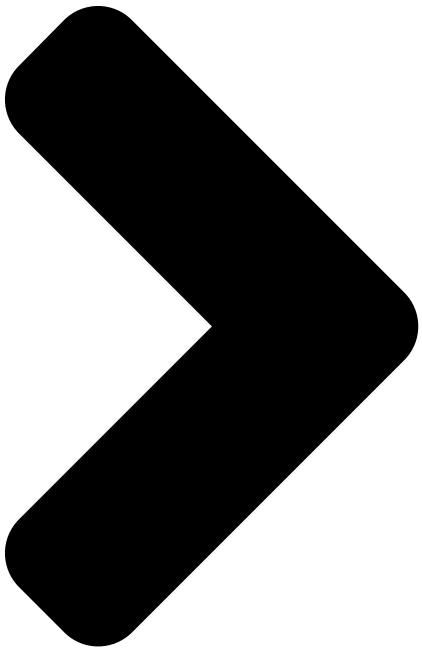
WordPress plugin TSI Careers

Trending Topic

Publicity

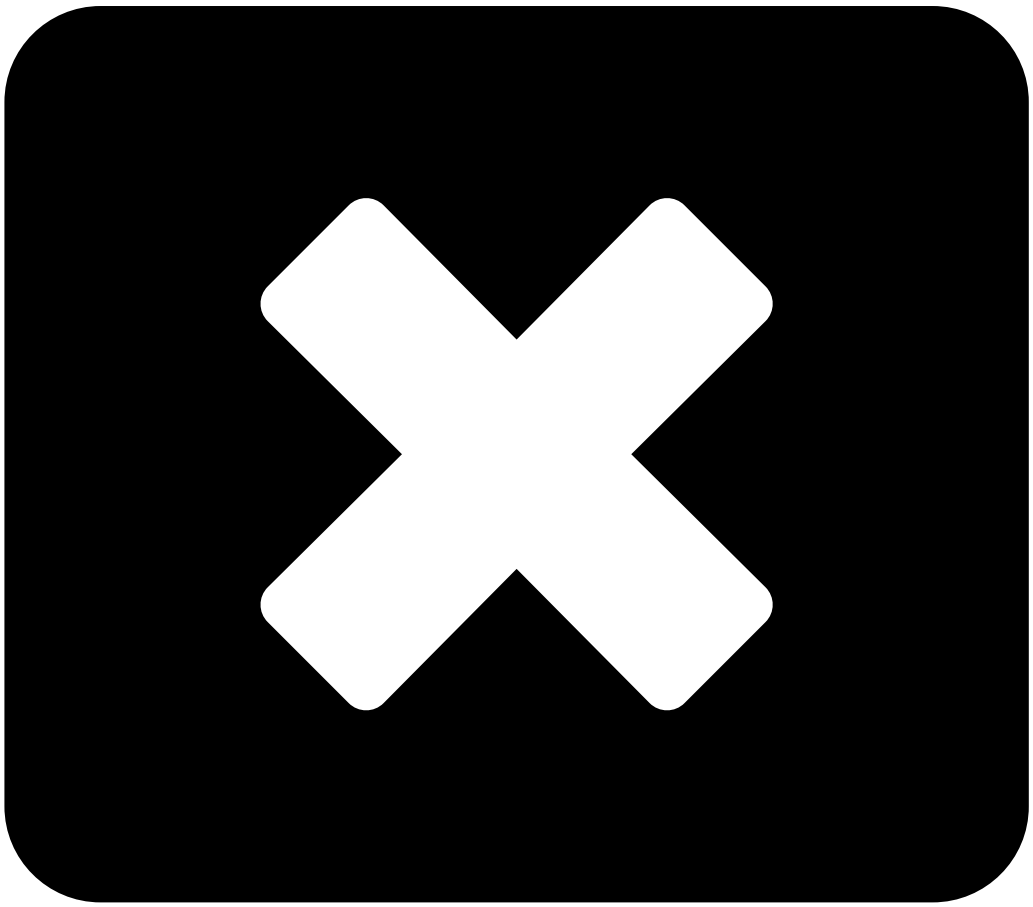
Interesting stuff to read


Digital Solution

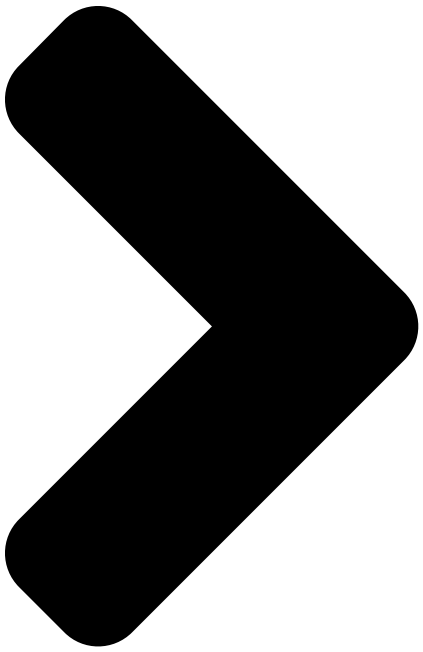


See More

Edit Template

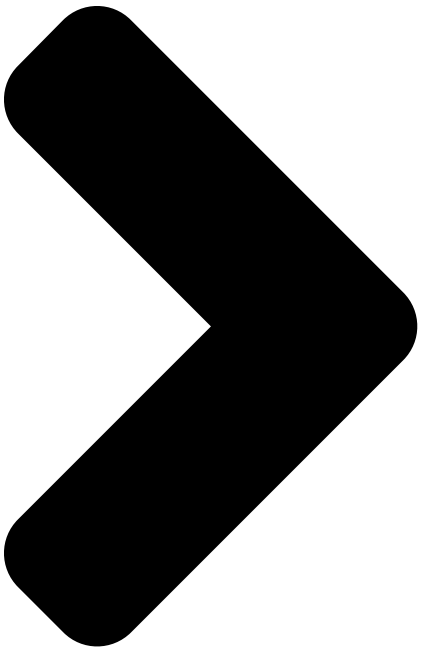


•



Blogs

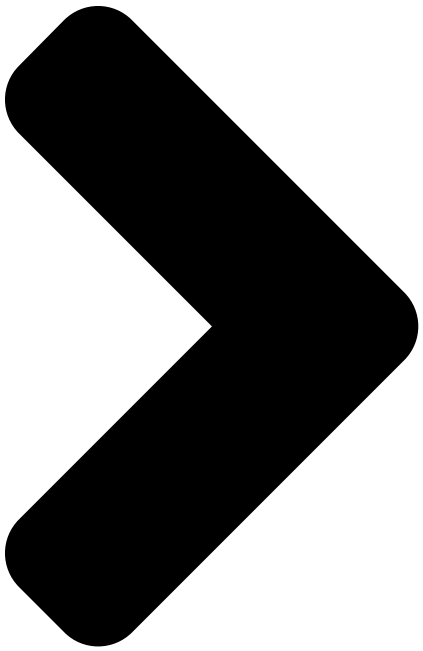
-



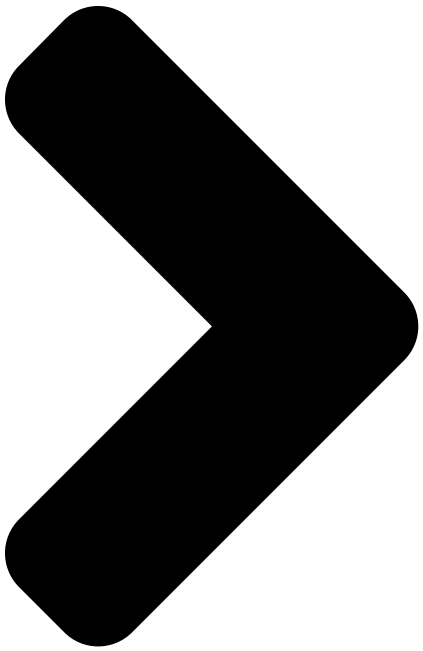
Request for detailed website quote

Some weekly posted topics

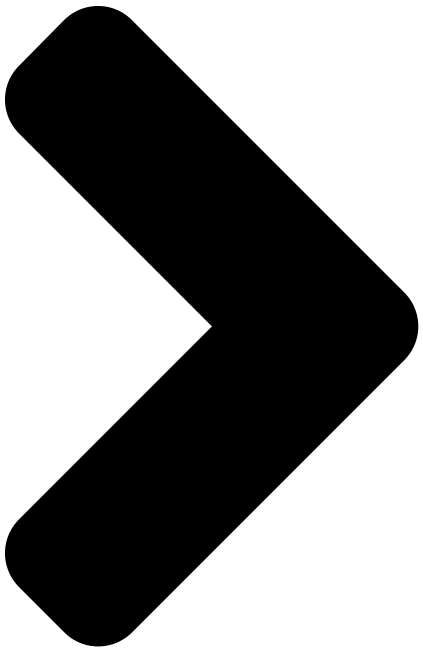
-



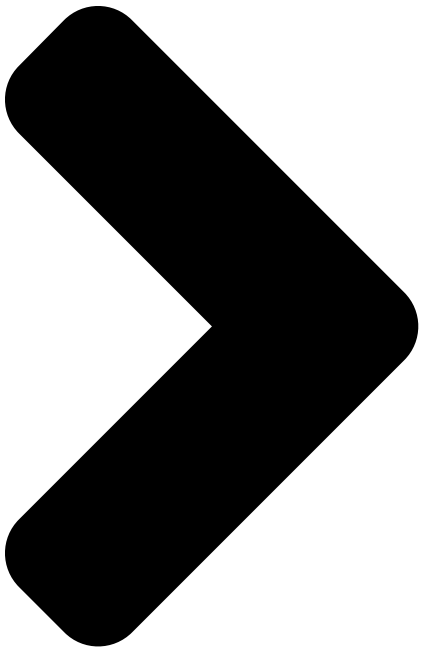
- Cheap Website vs. High Performance



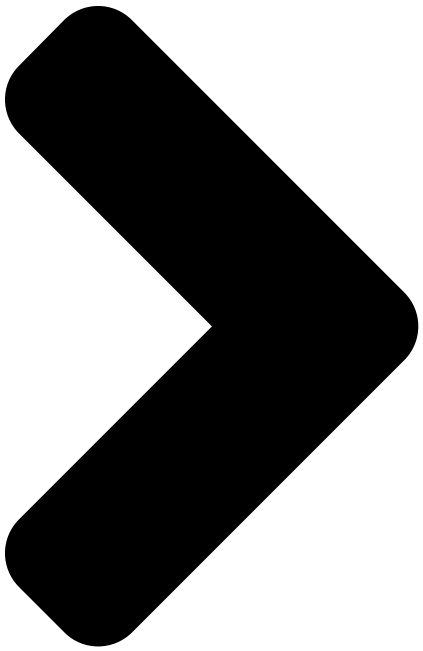
- What Is an AI Agent?



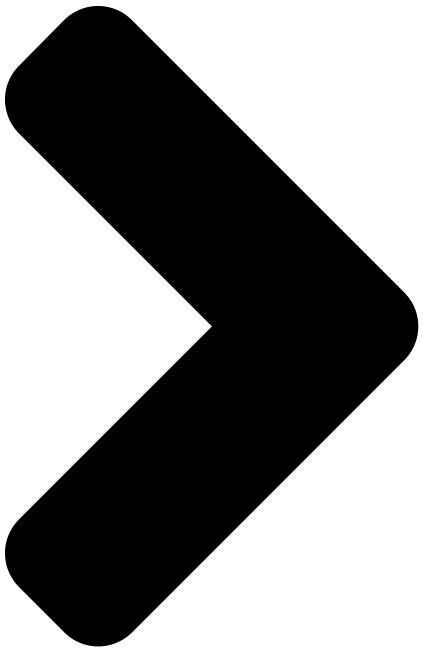
Client Communication in Digital Marketing



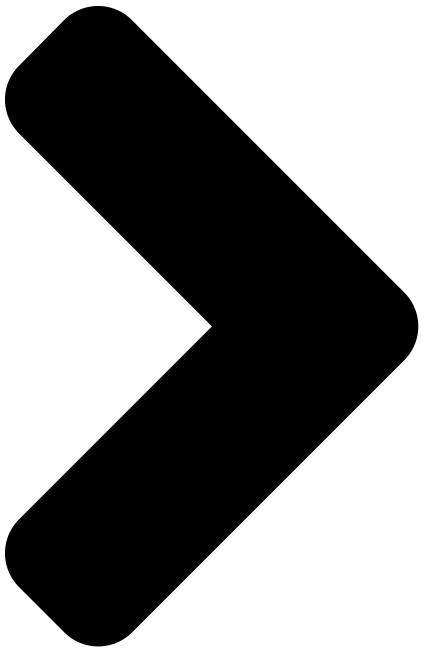
- Human Made Websites vs AI Websites



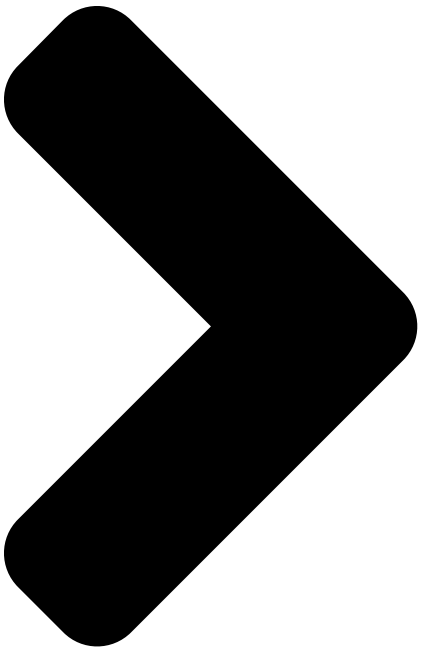
Your Digital Marketing Ecosystem Explained



- Mastering Answer Engine Optimization (AEO)



- Beware the Template Trap

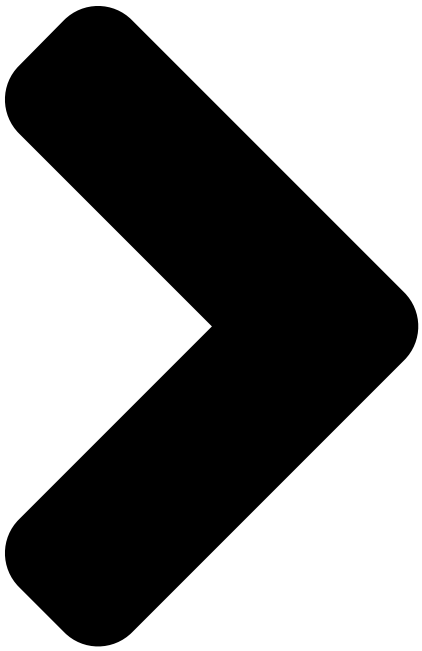


NWOW: Results Matter, Not Presence

Trending Topic

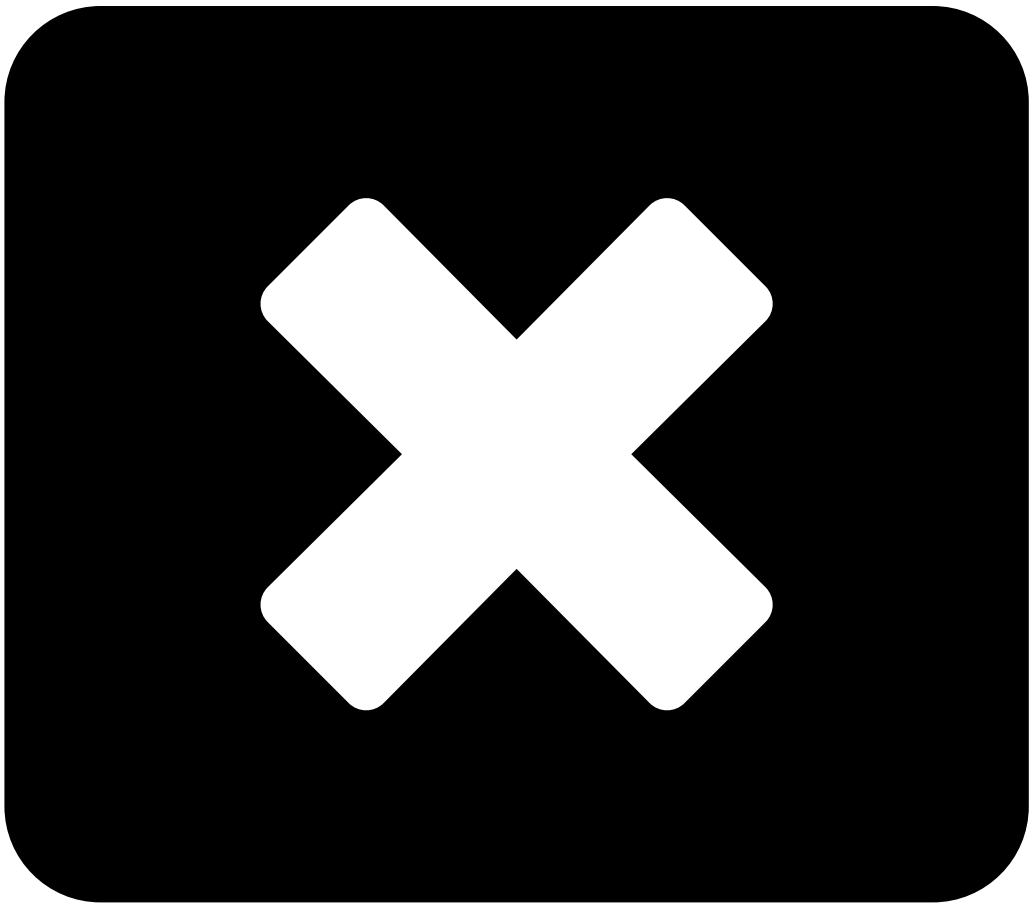
Publicity


Digital Solution

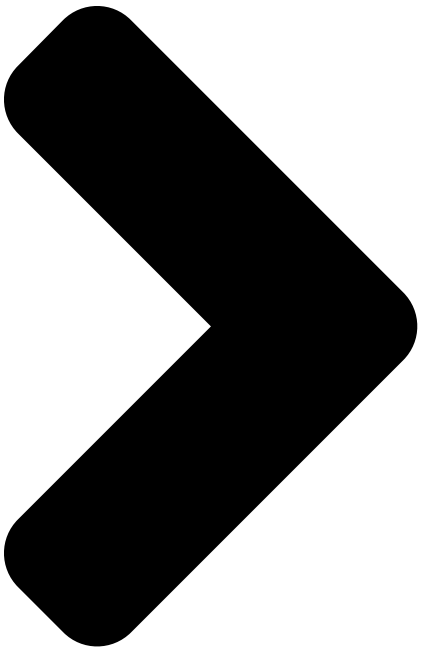


Who we are

Edit Template

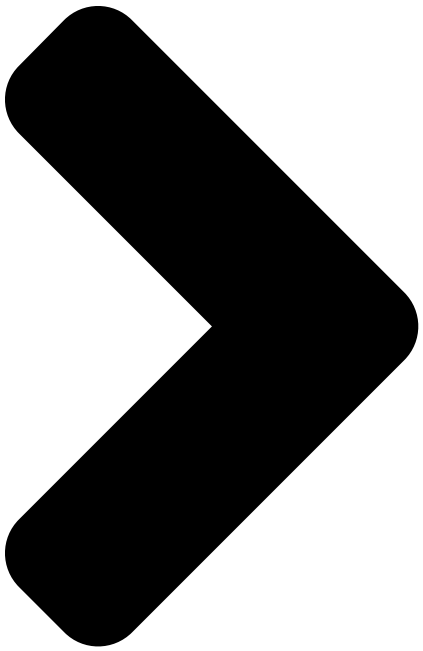


•

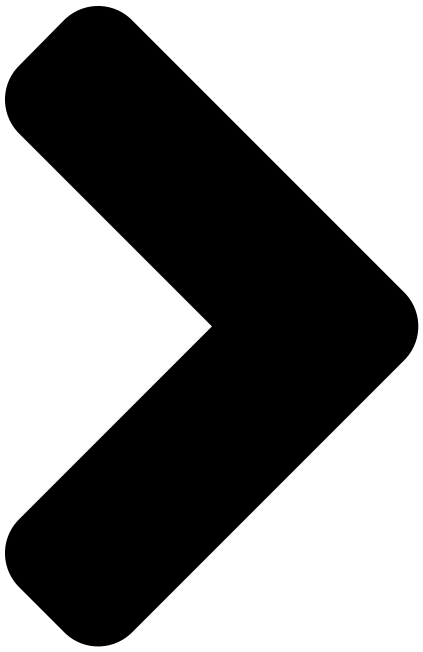


Contact us

-

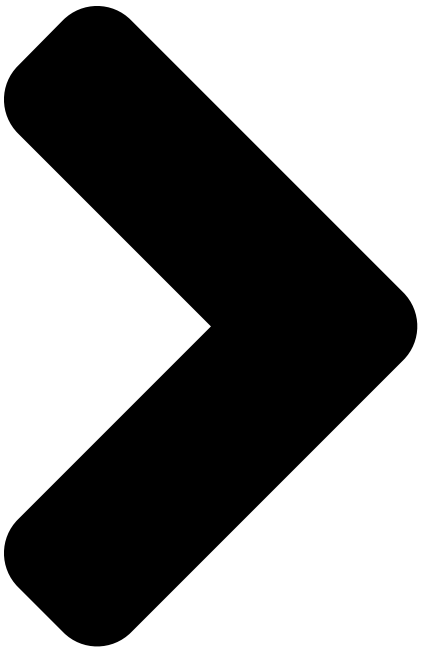


Request for detailed website quote



Jobs @ TSI Digital Solution

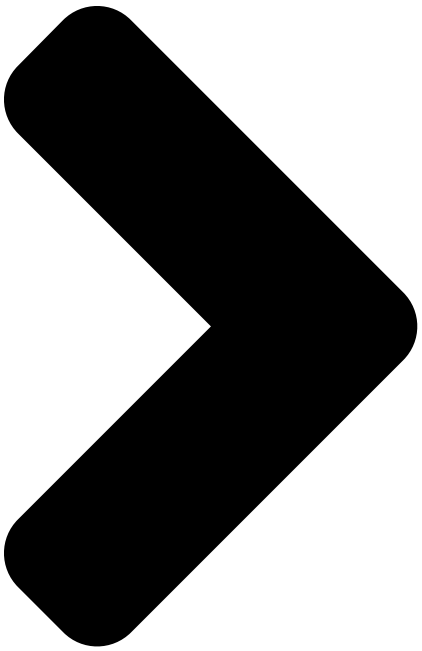
-



Affiliate program

Tools for free

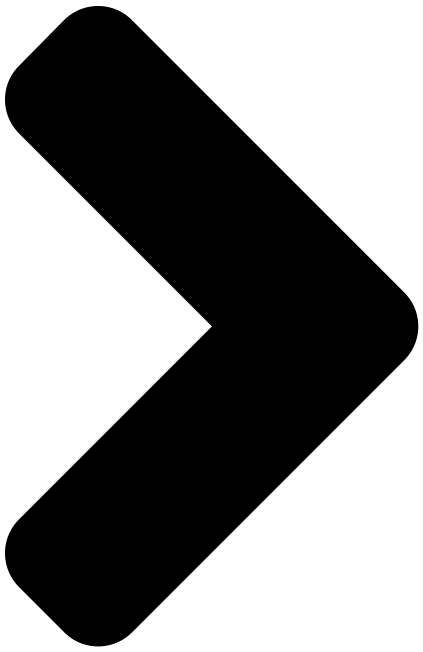
-



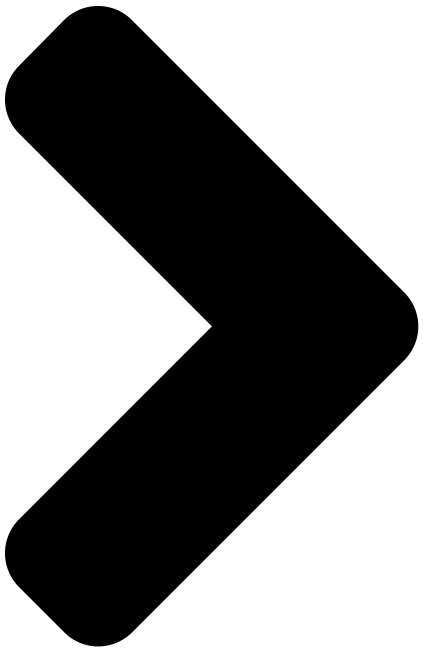
TSI Free Tools

WordPress plugins by TSI

-



TSI Visitor Blocker

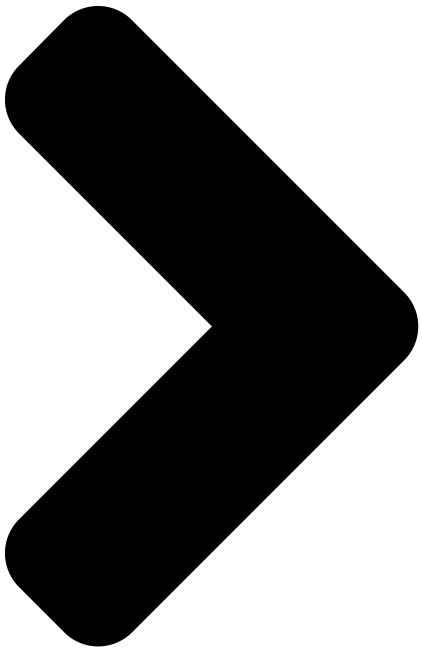


TSI Careers

Trending Topic

Publicity


Digital Solution



See More

Edit Template

Edit Template

Meta video selfie verification GDPR

Get An Online Quote

What About Your Privacy?

GDPR Risks, Biometric Data and Privacy Concerns

Meta is introducing increasingly sophisticated security measures to protect Facebook and Instagram users against impersonation, fraudulent accounts and

identity theft. One of these measures is video selfie verification, a technology designed to confirm that a real person is behind an account.

In times of artificial intelligence (AI), deepfakes and increasingly convincing online scams, the technology offers an obvious security benefit. But it also raises an important question: **what happens to your personal information when verifying your identity means sharing a video of your face with a global technology company?**

The Meta video selfie verification GDPR debate goes beyond account security. It raises important questions about biometric data processing, facial recognition, user consent, data retention and individual privacy rights under European data protection law.

Meta says it has implemented safeguards, including encryption and the deletion of facial data generated after verification. However, the existence of security measures does not automatically settle every question about GDPR compliance.

For individuals, the concern is control over personal information. For businesses, creators and digital marketing agencies, it is about maintaining customer trust and understanding the privacy implications of the platforms they rely on.

Understanding the relationship between Meta's video selfie verification, GDPR and biometric privacy is essential for anyone operating in today's increasingly regulated digital environment.

What Is Meta Video Selfie Verification and How Does It Work?

Meta's video selfie verification is an identity verification method that uses facial recognition technology to help people regain access to compromised Facebook and Instagram accounts.

Instead of relying exclusively on traditional identity documents, eligible users can upload a short video selfie. Meta then compares the face in the video with photographs associated with the account. The objective is to determine whether the individual attempting to recover the account is the legitimate account holder.

Meta announced its video selfie verification initiative in October 2024 and subsequently expanded its availability to the European Union, United Kingdom and South Korea in March 2025.

Is Meta Video Selfie Verification GDPR-Compliant?

Meta video selfie verification is not automatically illegal under GDPR. However, its use of facial recognition raises important data protection questions because biometric data processed to confirm an individual's

identity can fall under GDPR Article 9.

Meta states that uploaded video selfies are encrypted and that facial data generated during comparison is deleted when no longer needed. Nevertheless, organisations must consider the applicable legal basis, Article 9 conditions, transparency, data retention and security safeguards.

For businesses, the key lesson is that using biometric verification technology requires more than technical security. It requires appropriate legal justification, accountability and respect for individual privacy rights.

How Does the Verification Process Work?

The general process involves three stages:

1. **Video submission:** The user uploads a short video selfie through the account recovery process.
2. **Facial comparison:** Meta uses facial recognition technology to compare the submitted video with photographs associated with the account.
3. **Identity verification:** The comparison helps Meta determine whether the individual is likely to be the legitimate account holder.

What Does Meta Say About Data Protection?

According to Meta’s official announcement:

- Uploaded video selfies are encrypted and stored securely.
- Videos are not displayed on users’ profiles.
- Facial data generated after the comparison is immediately deleted, regardless of whether a match is identified.
- Video selfie verification is an optional account recovery method.

These safeguards are relevant when assessing Meta’s approach to privacy.

However, users should distinguish between the uploaded video and the facial data generated during the comparison. The company’s statement about deleting generated facial data does not necessarily mean that the original video is deleted at precisely the same time.

Official source: Meta – Testing New Ways to Combat Scams and Help Restore Access to Compromised Accounts

Why Does Meta Video Selfie Verification Raise GDPR Concerns?

The main GDPR concern is not simply that Meta collects a photograph or video containing someone’s face. It is how that information is technically processed and whether the resulting information qualifies as biometric data used for uniquely identifying an individual.

Under Article 4(14) GDPR, biometric data refers to personal data resulting from specific technical processing relating to a person’s physical, physiological or behavioural characteristics that allows or confirms their unique identification. Article 9 then provides additional protection for biometric data processed for the purpose of uniquely identifying a natural person.

This distinction matters because facial photographs do not automatically qualify as special-category biometric data. The purpose and technical processing determine whether the additional Article 9 protections apply.

GDPR Article 9 and Special-Category Biometric Data

Article 9 generally prohibits processing biometric data for uniquely identifying an individual unless an applicable exception exists.

These exceptions include:

- Explicit consent from the individual, where the relevant requirements are met.
- Certain processing activities necessary for legal obligations or rights.
- Specific substantial public interest grounds established by law.
- Other narrowly defined exceptions under Article 9.

Importantly, organisations must also identify an appropriate lawful basis under Article 6 GDPR where applicable.

This means that a business interest in preventing fraudulent accounts does not automatically establish permission to process biometric data. The legal basis and applicable Article 9 exception must be assessed separately.

Does Facial Recognition Automatically Violate GDPR?

No.

GDPR does not prohibit every use of facial recognition technology. It establishes conditions and safeguards governing how personal data, including biometric information, may be processed.

A facial recognition system may be legally permissible where the organisation can demonstrate compliance with the relevant legal requirements.

For Meta, the important questions concern the precise processing activities, the legal basis, the applicable Article 9 exception, transparency and the safeguards provided to users.

For businesses adopting similar technologies, the lesson is clear: security benefits do not remove the obligation to protect personal information.

Useful reference: GDPR Article 9 – Processing of Special Categories of Personal Data

Does Meta’s Optional Video Selfie Verification Provide Genuine Consent?

Meta describes video selfie verification as optional. Users can choose alternative identity verification methods where available.

However, the concept of optional participation raises a wider question: how freely can someone make a decision when they are trying to regain access to an account containing important business contacts, customer relationships or personal information?

Under Article 7 GDPR, consent must be freely given, specific, informed and unambiguous. Where Article 9 relies on explicit consent, the additional requirements must also be satisfied.

When Is Consent Considered Freely Given?

The GDPR requires organisations to consider the circumstances surrounding consent.

Relevant factors include:

- Whether users understand what personal information is collected.
- Whether the processing purpose is clearly explained.
- Whether **users can refuse without unnecessary disadvantages**.
- Whether **alternative options are genuinely available**.
- Whether consent can be withdrawn where it is the legal basis.

An organisation should not assume that a consent checkbox automatically makes processing lawful.

Can Legitimate Interest Justify Biometric Data Processing?

Legitimate interest is one of the lawful bases under Article 6 GDPR.

It may be relevant to certain fraud prevention and security activities. However, legitimate interest alone does not override Article 9’s restrictions on special-category biometric data. Where Article 9 applies, an organisation must also establish a relevant exception.

This is an important distinction for businesses using identity verification systems, customer authentication tools and AI-powered security technologies.

What Happens to Your Facial Data After Meta Verification?

Biometric information requires particularly careful protection because its characteristics are difficult or impossible to replace.

If a password is compromised, a user can create a new one. If biometric information is exposed, changing the underlying physical characteristic is

generally not a realistic option.

Meta says uploaded video selfies are encrypted and stored securely. It also states that facial data generated during the comparison is immediately deleted, regardless of whether the system identifies a match. However, responsible privacy analysis requires examining both the generated facial data and the original video.

Data Retention and Deletion

GDPR Article 5 establishes several principles relevant to biometric verification:

- Data minimisation.
- Purpose limitation.
- Storage limitation.
- Integrity and confidentiality.
- Accountability.

Organisations must ensure that personal information is retained only for as long as necessary for its intended purpose.

This raises practical questions for any organisation implementing facial recognition:

1. How long is the original video retained?
2. Who can access the uploaded information?
3. Is any information shared with third-party processors?
4. What happens when a user withdraws consent?
5. How are deletion requests handled?
6. What happens if a security breach occurs?

These questions should be addressed through clear privacy notices, documented retention policies and appropriate technical safeguards.

Why Biometric Data Breaches Can Be Particularly Serious

A biometric data breach can have long-term consequences. Facial information may be used in identity fraud, impersonation attempts and other forms of misuse. The difficulty of replacing biometric characteristics makes data minimisation and appropriate security controls especially important.

Businesses should therefore avoid collecting biometric information unless they have a clearly established purpose, appropriate legal grounds and suitable security arrangements.

Meta’s Privacy History: What Businesses Can Learn from Previous GDPR Cases

Meta has faced significant regulatory scrutiny concerning its handling of personal information.

These enforcement actions provide useful context for understanding why data protection should be treated as a fundamental business responsibility.

The €1.2 Billion GDPR Fine

In May 2023, Ireland’s Data Protection Commission imposed a €1.2 billion GDPR fine against Meta Platforms Ireland Limited.

The decision concerned the transfer of European Economic Area personal data to the United States and violations involving international data transfers.

It remains one of the most significant GDPR enforcement actions.

The $1.4 Billion Texas Biometric Settlement

In July 2024, Meta agreed to a $1.4 billion settlement with Texas over allegations involving the collection and use of biometric data under Texas law.

The case concerned Facebook’s historical facial recognition practices and its Tag Suggestions feature.

It is important to distinguish this settlement from Meta’s current video selfie verification process. The settlement should not be presented as a legal finding against that specific feature.

What Do These Cases Mean for Smaller Businesses?

Large technology companies have substantial resources to manage regulatory investigations and litigation. Smaller businesses may not have the same financial or operational capacity.

Under GDPR Article 83, certain infringements can attract fines of up to €20 million or 4% of the undertaking’s total worldwide annual turnover for the preceding financial year, whichever is higher.

For smaller organisations, privacy failures can also result in:

- Legal expenses.
- Customer complaints.
- Reputational damage.
- Operational disruption.
- Loss of customer confidence.

The important lesson is that GDPR compliance should be part of everyday business operations rather than something addressed only after a problem occurs.

How Does the EU AI Act Affect Biometric

Verification?

The General Data Protection Regulation is not the only European regulation relevant to facial recognition and artificial intelligence.

The EU Artificial Intelligence Act introduces additional requirements for certain AI applications, including specific biometric identification systems.

However, an important distinction must be made between biometric identification and biometric verification. Not every facial recognition application automatically qualifies as high-risk under the AI Act.

Biometric Identification vs Biometric Verification

Biometric identification generally involves identifying an individual by comparing biometric information against a reference database. Biometric verification, sometimes called authentication, involves confirming that a specific person is the individual they claim to be. The AI Act distinguishes between these applications.

Certain remote biometric identification systems are classified as high-risk under Annex III.

However, biometric verification systems whose sole purpose is confirming that a specific individual is the person they claim to be are treated differently under the relevant classification framework. This distinction is particularly important when assessing account recovery systems such as Meta’s video selfie verification.

Important EU AI Act Compliance Dates

As of November 2026, the revised EU AI Act implementation framework includes the following milestones:

Date	Regulatory milestone
1 August 2024	AI Act entered into force
2 February 2025	Prohibited AI practices and AI literacy provisions began applying
2 August 2025	General-purpose AI model obligations and governance provisions began applying
2 August 2026	Most AI Act provisions became applicable
2 December 2027	Relevant Annex III high-risk AI requirements become applicable
2 August 2028	Relevant Annex I high-risk AI requirements become applicable

The revised dates follow the AI Omnibus amendments that entered into force in July 2026.

Businesses should not interpret these dates as a blanket deadline for every organisation using facial recognition technology. The applicable obligations depend on the AI system’s classification and the organisation’s role.

What Should Businesses Do Now?

Businesses developing or deploying AI systems should:

- Assess the intended purpose of each AI system.
- Determine whether the system falls within a high-risk category.
- Review relevant documentation and risk management obligations.
- Establish appropriate human oversight where required.
- Review data protection and security arrangements.
- Monitor regulatory guidance and implementation developments.

Even where the AI Act's high-risk provisions do not apply, GDPR obligations may still be relevant.

Official reference: European Commission – AI Act Regulatory Framework

What Does Meta Video Selfie Verification Mean for Businesses and Digital Marketers?

Businesses frequently rely on Facebook and Instagram for advertising, customer acquisition, lead generation and brand development. However, the privacy implications of modern digital platforms extend beyond the information businesses directly collect from their customers.

Marketing operations frequently involve advertising platforms, analytics tools, CRM systems, automation software and third-party integrations. Understanding how these technologies process personal information is essential for responsible digital marketing.

Build a First-Party Data Strategy

First-party data allows businesses to establish direct relationships with customers through channels they control.

Examples include:

- Permission-based email marketing.
- Customer relationship management systems.
- Website contact forms.
- Customer loyalty programmes.
- Direct customer communities.

A well-managed first-party data strategy can reduce unnecessary dependence on external platforms while improving customer relationships.

Review Your Consent Mechanisms

Businesses should ensure that their lead generation forms and marketing communications explain how personal information is collected and used. Consent should be specific and meaningful wherever it is used as the legal basis for processing.

Organisations should also provide suitable mechanisms for withdrawing consent and maintain appropriate records.

Audit Third-Party Marketing Tools

Modern marketing operations often depend on multiple third-party technologies.

Businesses should periodically review:

- What information each tool collects.
- Whether information is shared with other organisations.
- Whether international data transfers occur.
- How information is stored and protected.
- Whether appropriate contractual arrangements exist.

This process helps businesses understand where privacy risks may arise.

Diversify Your Digital Marketing Channels

Relying entirely on one social media platform creates unnecessary business risks.

A sustainable digital marketing strategy should combine:

- Search engine optimisation.
- Social media marketing.
- Website content marketing.
- Email marketing.
- Paid advertising.
- Direct customer engagement.

The objective is not to abandon Meta. It is to create a digital presence that remains resilient when individual platforms change their policies, algorithms or operating practices.

Why Privacy-First Marketing Can Become a Competitive Advantage

Privacy compliance is frequently viewed as an additional business expense.

However, organisations that demonstrate responsible data practices can create a meaningful competitive advantage. Customers increasingly expect brands to explain how their personal information is collected, stored and used. A company that communicates these practices clearly can build stronger relationships and differentiate itself from competitors that treat privacy as an afterthought.

Greater Customer Confidence

Transparent privacy notices and responsible information collection help customers understand what happens to their personal data.

This can make customers more comfortable interacting with a brand.

Stronger Brand Reputation

Businesses that demonstrate accountability can strengthen their credibility with customers, partners and stakeholders.

Privacy-conscious practices can become part of a brand’s wider reputation for professionalism and trustworthiness.

Reduced Compliance Risks

Data minimisation, appropriate consent mechanisms and regular audits help organisations identify potential problems before they escalate.

More Sustainable Digital Marketing

A first-party data strategy gives businesses greater control over customer relationships and reduces excessive dependence on external platforms.

Privacy-first marketing is therefore not simply about avoiding regulatory penalties. It is about building a digital business that customers have good reasons to trust.

What Are the Risks of Ignoring GDPR and Data Protection?

Ignoring data protection obligations can create serious operational and reputational problems. Businesses that collect unnecessary personal information, use unclear consent mechanisms or fail to protect customer information may expose themselves to regulatory scrutiny.

For digital marketing agencies, the situation requires particular attention. Agencies may manage campaigns, customer databases, tracking technologies, websites and lead generation systems on behalf of their clients.

Depending on the actual processing activities and contractual arrangements, an agency may act as a controller, processor or joint controller.

Each role has different responsibilities under GDPR.

Legal and Financial Exposure

Inadequate data protection practices can result in regulatory investigations, complaints and financial penalties.

Businesses should understand their legal obligations before introducing new technologies or collecting additional categories of personal information.

Loss of Customer Trust

Customers may reconsider their relationship with a brand if they believe

their personal information has been handled irresponsibly.

Rebuilding trust after a serious privacy incident can be difficult.

Operational and Reputational Damage

A data breach or regulatory investigation can disrupt normal business activities and damage brand reputation.

For agencies, these problems may also affect client relationships and future business opportunities.

The strongest approach is preventative rather than reactive. Organisations should identify privacy risks before implementing new technologies rather than waiting for complaints or investigations.

Conclusion: Your Customers’ Privacy Is Part of Your Brand Reputation

Meta’s video selfie verification highlights an important challenge facing the modern digital economy.

As artificial intelligence makes online impersonation, identity theft and fraudulent accounts increasingly sophisticated, biometric verification technologies will likely become more common. These technologies can offer genuine security benefits. However, convenience and security should not come at the expense of transparency, accountability and individual privacy rights.

The GDPR establishes important safeguards for biometric information, while the EU AI Act introduces additional obligations for specific AI applications. For businesses and digital marketers, the practical lesson is clear: do not outsource your entire privacy strategy to the platforms you use.

Understand the technologies behind your marketing operations. Review your data collection practices. Make consent meaningful. Build direct customer relationships and work with partners who take privacy seriously.

At TSI Digital Solution, we believe the future of digital marketing belongs to brands that combine intelligent growth strategies with responsible data practices.

The strongest digital presence is not simply the one that attracts the most attention. It is the one that earns and maintains customer trust.

TSI Digital Solution’s Perspective: Privacy Must Be Part of Digital Growth

At TSI Digital Solution, we believe digital marketing performance should never come at the expense of customer trust.

Businesses often focus on website traffic, advertising performance, lead

generation and conversion rates. However, responsible data collection and transparent customer communication deserve the same strategic attention.

Our practical recommendation is to evaluate every marketing technology according to three questions:

1. **Necessity:** Does the technology genuinely require the personal information being collected?
2. **Transparency:** Can customers clearly understand how their information is being used?
3. **Accountability:** Can the business demonstrate that appropriate safeguards and responsibilities are in place?

These principles help businesses make more informed technology decisions while building stronger customer relationships.

Privacy should not be treated as a marketing obstacle. It should be part of the foundation of a sustainable digital strategy.

Business Checklist: 7 Steps to Improve Biometric Data Privacy

Businesses introducing identity verification or other biometric technologies should consider the following:

☐ Identify exactly what biometric information the technology collects.

☐ Establish the applicable GDPR Article 6 lawful basis.

☐ Identify an applicable Article 9 exception where special-category biometric data is processed.

☐ Review whether a Data Protection Impact Assessment (DPIA) is required.

☐ Establish transparent retention and deletion policies.

☐ Review third-party processors, contracts and security arrangements.

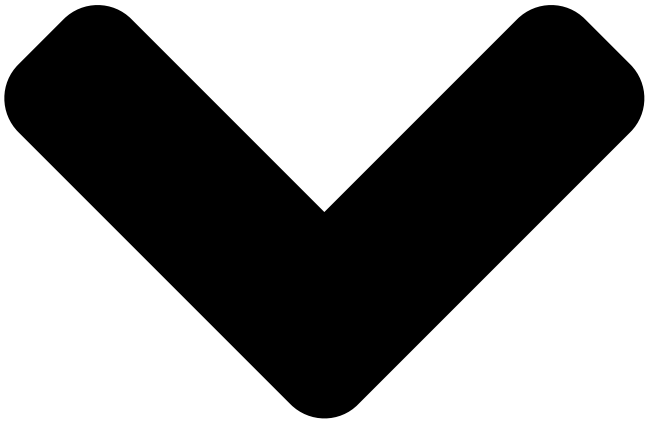
☐ Provide appropriate information about individual data protection rights.

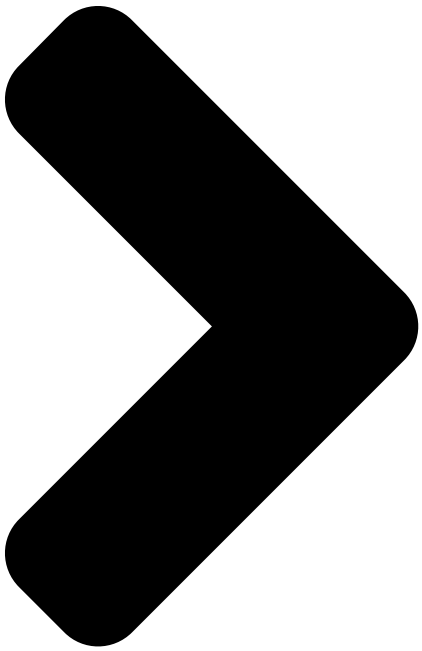
Important: A DPIA is mandatory where processing is likely to result in a high risk to individuals' rights and freedoms. Biometric processing for identification is specifically highlighted by European supervisory guidance as requiring particular attention. Organisations should assess their actual processing activities and applicable national requirements.

For further guidance, consult the Dutch Data Protection Authority's biometric data guidance.

Frequently Asked Questions (FAQ)

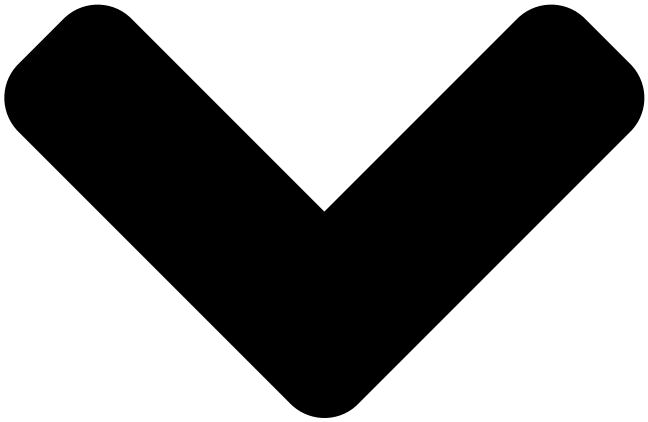
Is Meta video selfie verification illegal under GDPR?

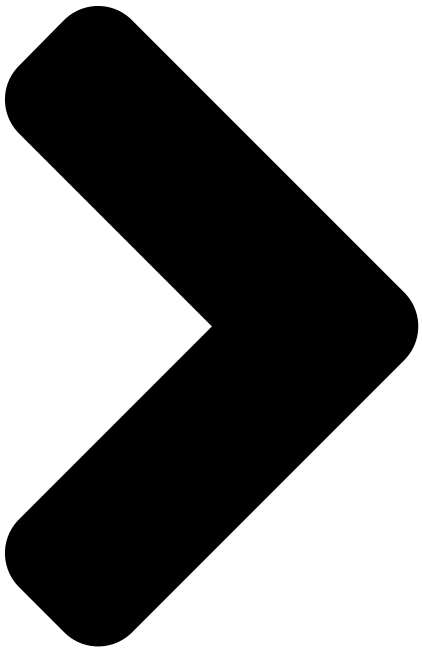




Not automatically. Meta’s video selfie verification raises questions about biometric data processing, transparency, consent and the legal basis for processing. Whether a particular implementation complies with GDPR depends on its actual processing activities and the applicable legal requirements. There is no basis for declaring the feature definitively illegal simply because it uses facial recognition technology.

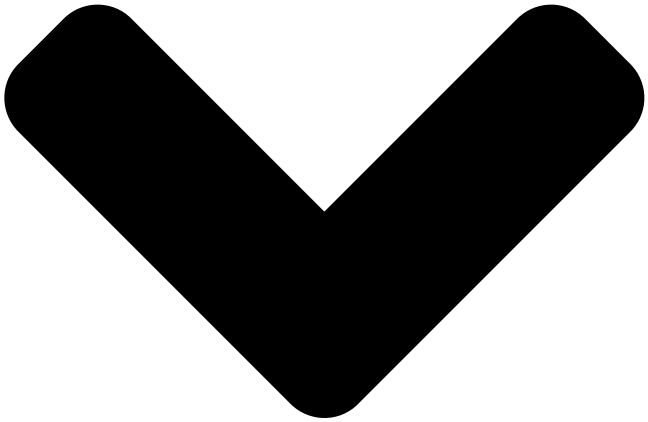
Does Meta collect biometric data through video selfie verification?

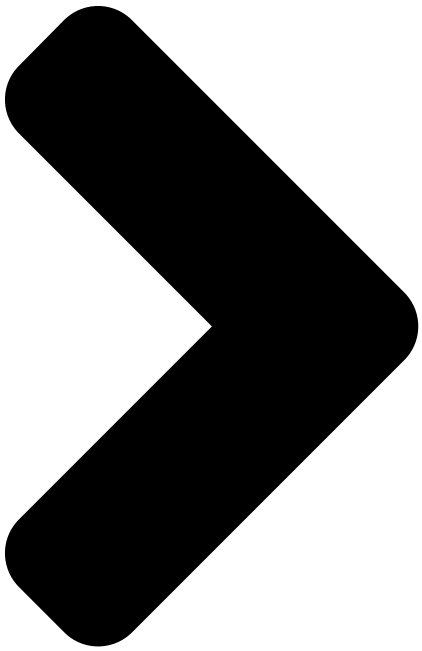




Meta uses facial recognition technology to compare an uploaded video selfie against photographs associated with an account. Where specific technical processing produces biometric data for uniquely identifying an individual, GDPR Article 9 may apply. An ordinary facial photograph does not automatically qualify as special-category biometric data.

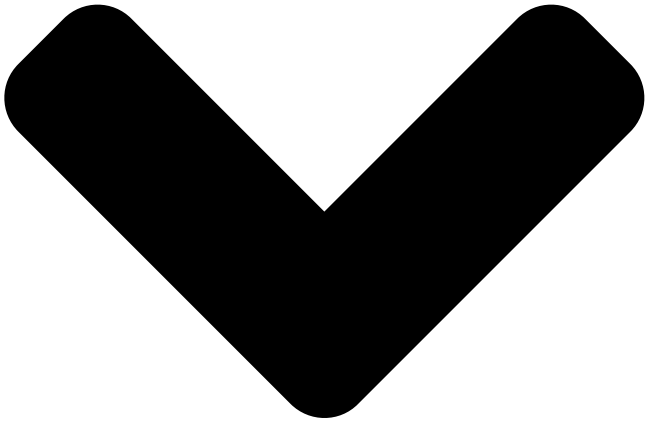
What happens to my video selfie after Meta verification?

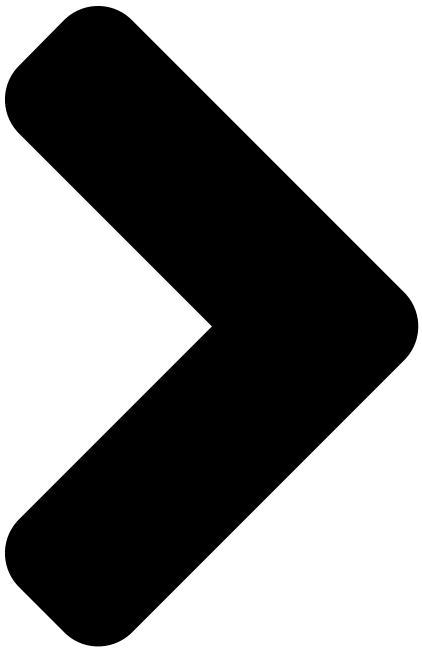




Meta states that uploaded video selfies are encrypted and stored securely. It also says facial data generated after the comparison is immediately deleted, regardless of whether a match is identified. The uploaded video and the generated facial data are distinct, so users should consult Meta’s applicable privacy disclosures for information about video retention.

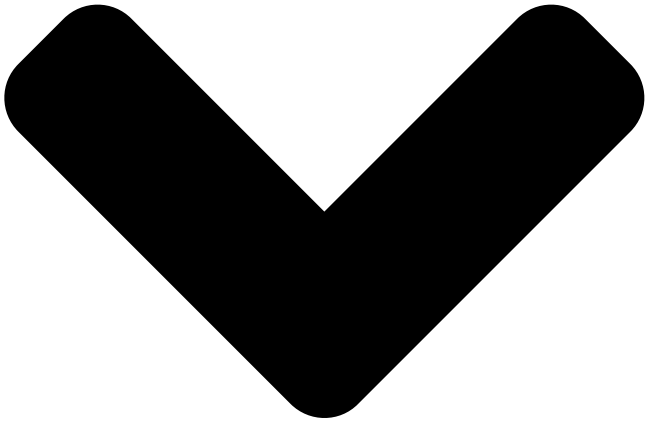
Can Meta use video selfie data for advertising?

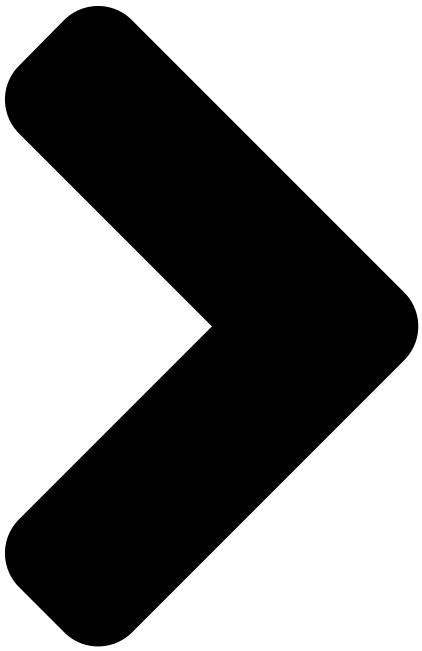




Meta’s published explanation of this account recovery feature describes using the video selfie to compare the user’s face with photographs associated with the account. It states that facial data generated after the comparison is deleted. This should not be confused with every other facial recognition or advertising-related activity across Meta’s platforms. Users should consult the relevant privacy notices for the processing purposes applicable to their circumstances.

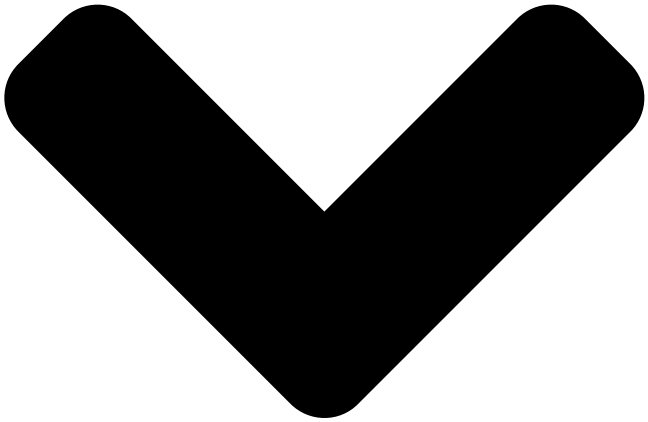
Does GDPR require explicit consent for biometric data?

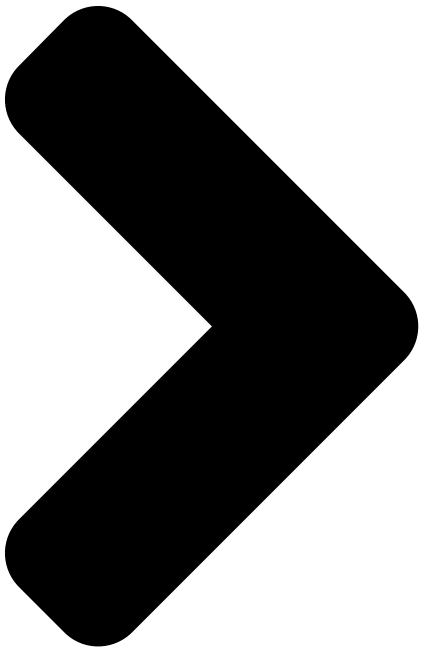




Article 9 generally prohibits processing biometric data for uniquely identifying an individual unless a recognised exception applies. Explicit consent is one possible exception, but it is not the only one. Organisations must also establish an appropriate lawful basis under Article 6 GDPR. Legitimate interest alone does not override Article 9 restrictions.

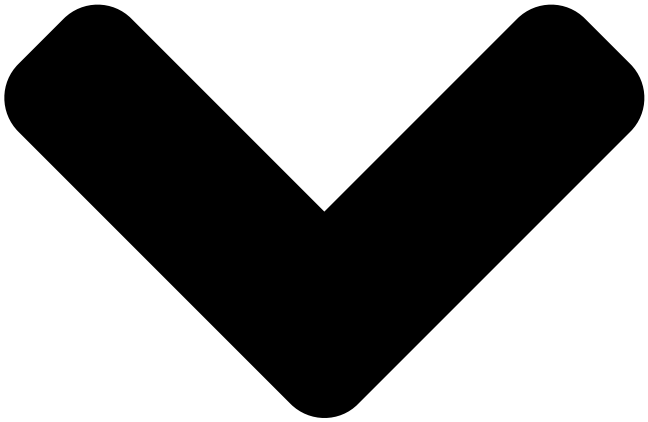
Is facial recognition considered high-risk under the EU AI Act?

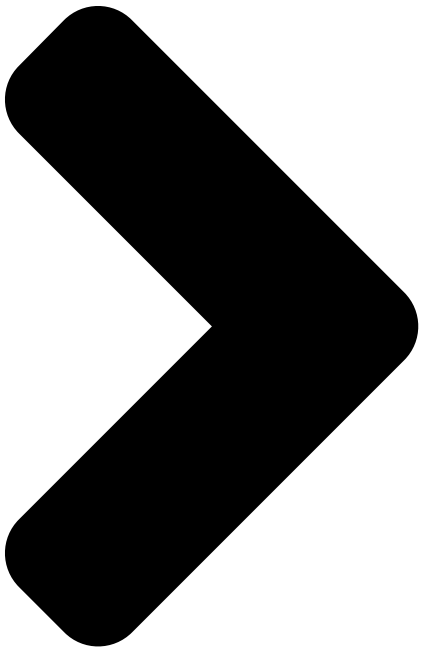




Some biometric identification systems are classified as high-risk under the EU AI Act. However, classification depends on the intended purpose and functionality. Certain biometric verification systems used solely to confirm a claimed identity are treated differently under the relevant Annex III provisions. Each system should be assessed individually.

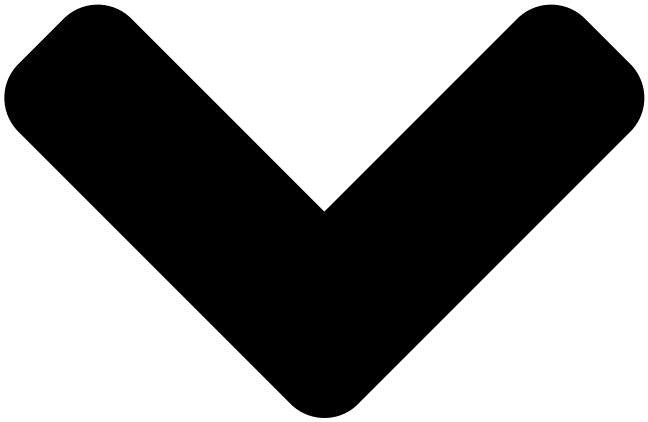
What can small businesses do to protect customer data?

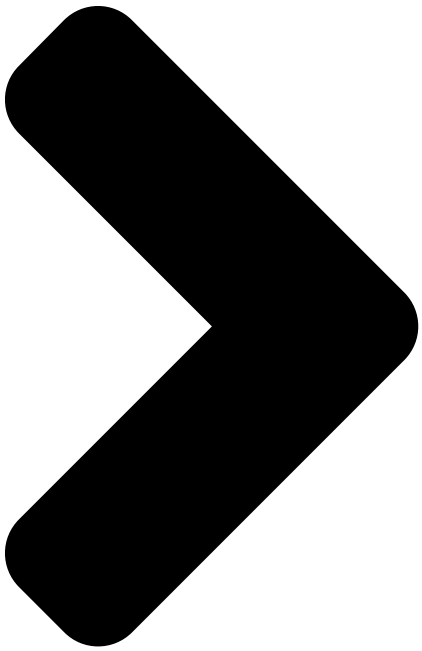




Small businesses should collect only necessary personal information, implement appropriate consent mechanisms, review third-party marketing tools, maintain suitable security measures and establish transparent privacy notices. They should also develop first-party marketing channels such as permission-based email lists and direct customer communities.

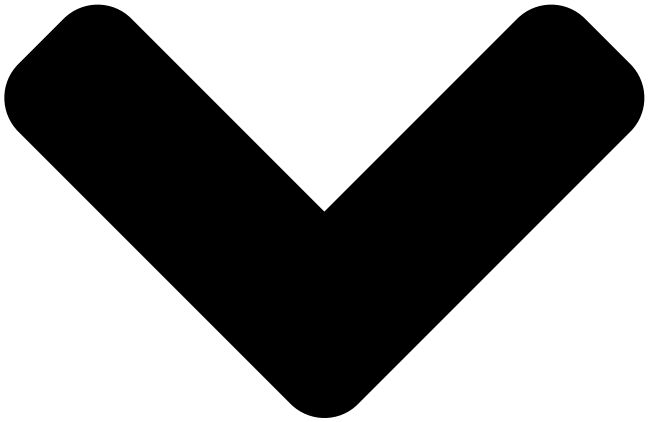
How can digital marketing agencies help businesses with privacy-conscious marketing?

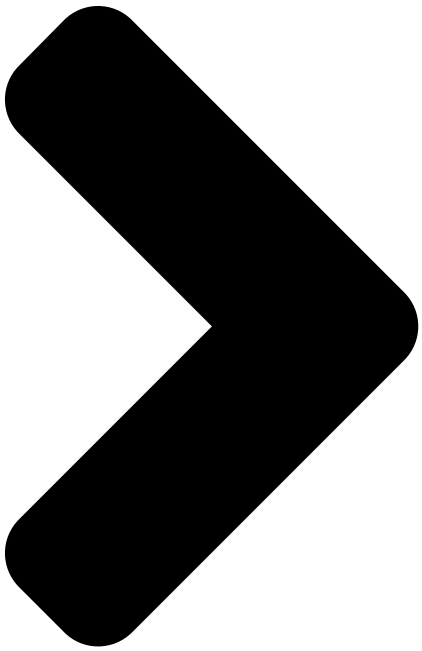




Digital marketing agencies can help businesses review marketing tools, implement transparent lead generation processes, diversify acquisition channels and develop privacy-conscious content and engagement strategies. Where legal interpretation or complex data processing activities are involved, qualified data protection professionals should be consulted.

How does TSI Digital Solution support privacy-conscious marketing?





TSI Digital Solution helps businesses develop sustainable digital marketing strategies through SEO, content marketing, social media management, lead generation and digital strategy. Our approach encourages transparent customer engagement, responsible data collection and long-term brand development.

Not automatically. Meta’s video selfie verification raises questions about biometric data processing, transparency, consent and the legal basis for processing. Whether a particular implementation complies with GDPR depends on its actual processing activities and the applicable legal requirements. There is no basis for declaring the feature definitively illegal simply because it uses facial recognition technology.

Meta uses facial recognition technology to compare an uploaded video selfie against photographs associated with an account. Where specific technical processing produces biometric data for uniquely identifying an individual, GDPR Article 9 may apply. An ordinary facial photograph does not automatically qualify as special-category biometric data.

Meta states that uploaded video selfies are encrypted and stored securely. It also says facial data generated after the comparison is immediately deleted, regardless of whether a match is identified. The uploaded video and the generated facial data are distinct, so users should consult Meta’s applicable privacy disclosures for information about video retention.

Meta’s published explanation of this account recovery feature describes using the video selfie to compare the user’s face with photographs associated with the account. It states that facial data generated after the comparison is deleted. This should not be confused with every other facial recognition or advertising-related activity across Meta’s platforms. Users should consult the relevant privacy notices for the processing purposes applicable to their circumstances.

Article 9 generally prohibits processing biometric data for uniquely identifying an individual unless a recognised exception applies. Explicit consent is one possible exception, but it is not the only one. Organisations must also establish an appropriate lawful basis under Article 6 GDPR. Legitimate interest alone does not override Article 9 restrictions.

Some biometric identification systems are classified as high-risk under the EU AI Act. However, classification depends on the intended purpose and functionality. Certain biometric verification systems used solely to confirm a claimed identity are treated differently under the relevant Annex III provisions. Each system should be assessed individually.

Small businesses should collect only necessary personal information, implement appropriate consent mechanisms, review third-party marketing tools, maintain suitable security measures and establish transparent privacy notices. They should also develop first-party marketing channels such as permission-based email lists and direct customer communities.

Digital marketing agencies can help businesses review marketing tools, implement transparent lead generation processes, diversify acquisition channels and develop privacy-conscious content and engagement strategies. Where legal interpretation or complex data processing activities are involved, qualified data protection professionals should be consulted.

TSI Digital Solution helps businesses develop sustainable digital marketing strategies through SEO, content marketing, social media management, lead generation and digital strategy. Our approach encourages transparent customer engagement, responsible data collection and long-term brand development.

Reach Out to Us

Ready to grow your business with a smarter and more responsible digital marketing strategy?

At TSI Digital Solution, we help businesses strengthen their online presence through strategic SEO, social media marketing, content creation, website optimisation and digital growth solutions.

Build a brand that attracts customers, earns trust and grows sustainably.

Contact TSI Digital Solution today to discuss your digital marketing strategy.

Leave a Reply

Logged in as TSI Digital Solution. Edit your profile. Log out? Required fields are marked *

Message*

Post Comment

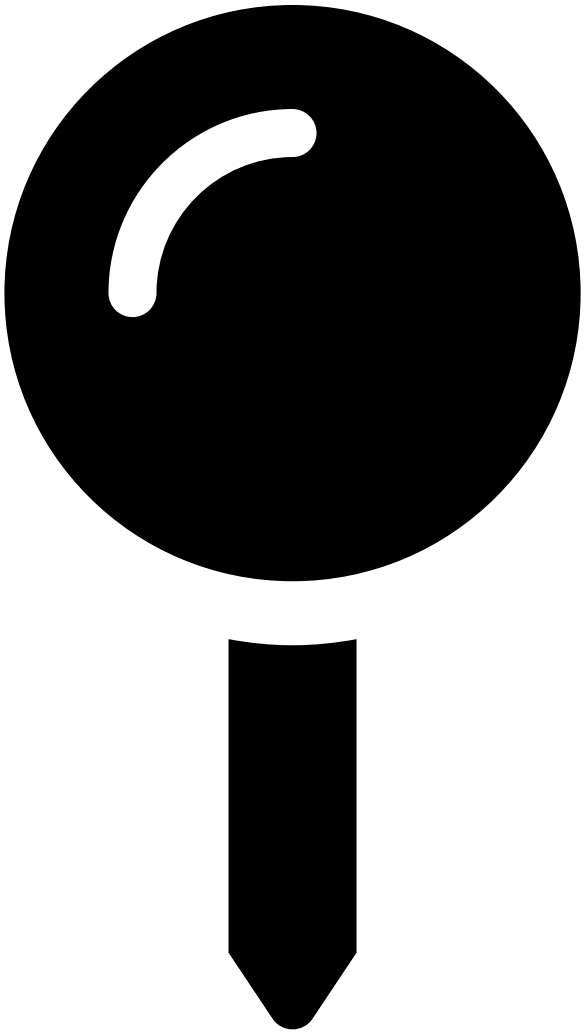
Go Back >

Get in Touch



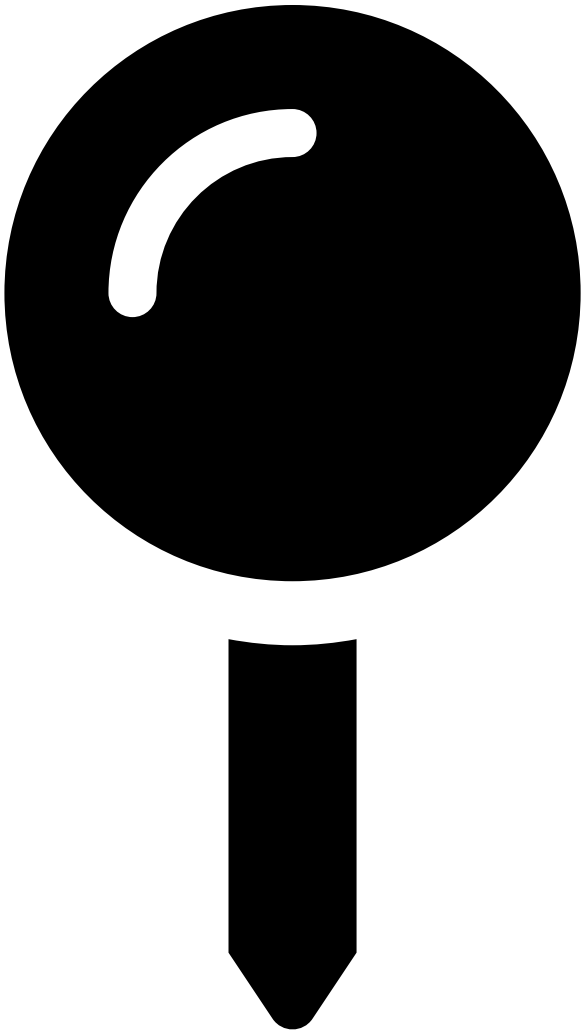
We Reflect Your Wishes

Contact



TSI Digital Solution
(Brand of PT Tripple SoRa Indonesia)

Jl. Sunset Road No.815 Seminyak, Kuta, Badung, Bali – 80361, Indonesia

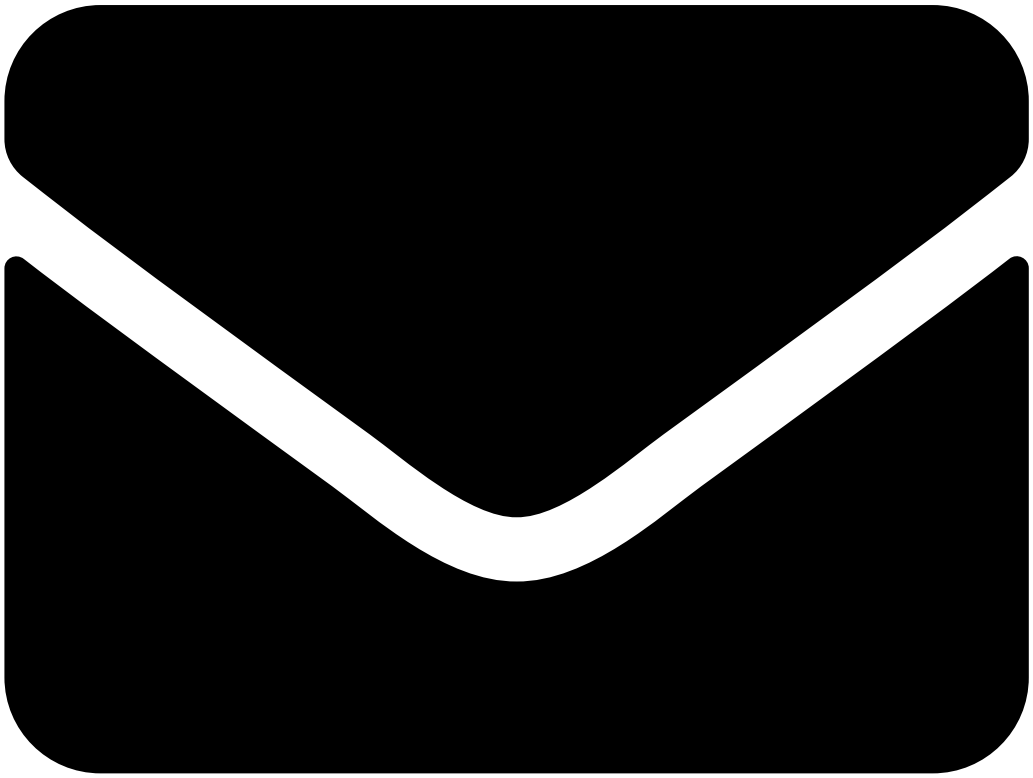


TSI Digital Solution
(Brand of PT Tripple SoRa Indonesia)

Jl. Sunset Road No.815 Seminyak, Kuta, Badung, Bali – 80361, Indonesia



+(62) 813-3936-1507



contact@tsidigitalsolution.com

Services

- Website/e-Commerce
- Apps
- AI Agents
- Technical/SEO
- Branding
- Social Media
- Graphic Design

- Copywriting
- Photo-& Videography



tsidigitalsolution.com
tsidigitalsolution.be
tsidigitalsolution.nl

Copyright © 2022 –

TSI Digital Solution | All rights reserved.

Edit Template