Online Dating & Discovery Association

TORO

Supply chain security and what it means for platforms handling sensitive user data

Many online dating and discovery platforms still focus most of their security effort on internal systems. While that remains essential, it no longer reflects where a growing number of incidents now originate - the supply chain.

As age assurance, trust and safety work and user support operations increasingly rely on third-party providers, sensitive data is often stored and processed outside the core platform.

In practice, your attack surface is no longer defined by your own infrastructure it is defined by the least protected part of your supply chain.

The Discord incident

A recent incident at Discord illustrates this point clearly. Discord itself was not breached. A third-party customer support vendor was compromised, which gave an attacker access to a subset of support tickets. For some users, those tickets included identity documents submitted during age-related appeals.

Discord removed the vendor's access and began notifying affected users, but the key lesson is still the same, users will not distinguish between a platform and its suppliers when their data is exposed.

Dating and discovery services face this reality on a daily basis. Verification data and trust-and-safety artefacts often sit with external providers, yet the platform will still be held responsible if something goes wrong.

Why supply chain risk is growing

From our work across the sector, three trends explain the rapid rise in supply chain exposure:

1. More sensitive data sits with third parties

Suppliers now routinely handle:

- Identity documents
- Age-verification artefacts
- User incident reports

- Fraud and behavioural signals

2. Vendor ecosystems have expanded

Platforms now rely on:

- Outsourced support teams
- Identity and age-assurance providers
- Moderation and trust-and-safety tools
- Cloud hosting and logging services
- CRM, ticketing and analytics platforms

Each brings its own set of risks.

3. Regulation requires increased data collection

Age-assurance and online-safety requirements is leading to more data being gathered, stored and transmitted often through external providers.

Where we see the most common weaknesses

Several issues appear repeatedly:

Unclear data flows

Many teams know who their vendors are, but not where sensitive data actually sits, which sub-processors are involved, or how long information is retained.

Sensitive data is spread across multiple systems

Identity documents are often uploaded into general support tools, duplicated in CRM systems or left in archives far longer than required.

Overly-broad access

Large numbers of internal and external staff can sometimes access personal information, often with limited monitoring.

Superficial supplier assurance

Contract clauses and certifications are used as a proxy for actual security. They rarely reflect how the supplier protects the specific data in use.

Online Dating & Discovery Association

TORO

Strengthening the supply chain

Improving supply chain security is not about adding one new control. It is about tightening core disciplines across the board:

1. Maintain a clear supplier and data map

This should show:

- What data each supplier processes
- Where it is stored
- Who can access it
- Which sub-processors are involved
- Retention and deletion practices

This includes understanding your entire supply chain, not just the top tier. Small vendors, niche providers or unmanaged SaaS platforms can create the same level of risk as your largest suppliers. Without visibility, protecting your data becomes guesswork.

2. Set minimum expectations for high-risk suppliers

These should cover access control, authentication strength, encryption, detailed logging, targeted testing and defined incident-notification requirements. Security certifications such as ISO 27001 or Cyber Essentials do not provide full assurance, but they are useful indicators of a supplier's maturity and commitment.

3. Limit what suppliers can see

Support teams generally need the outcome of an age check, not the underlying document. Reducing the data shared reduces the impact of any breach.

4. Avoid single points of dependency

Critical services should have viable alternatives and clear off-boarding routes, including verified data-return and deletion processes. A supplier you cannot replace becomes both an operational and security risk.

5. Treat supplier breaches as a standard scenario

Incident response plans should clearly define:

- How to identify affected users quickly
- How investigations are coordinated with suppliers
- How to handle regulatory and user notifications

- When to suspend a supplier's service
- What changes follow the incident

Being prepared changes the outcome.
Even well-managed suppliers will experience incidents. The difference is how quickly you can identify the impact and act.

6. Integrate people, processes and physical security

Technology is only one part of supply chain security. It depends on:

- How people handle data
- How processes govern access
- How physical and digital controls align

Human error remains one of the most common causes of supply chain exposure.

7. Keep communication open

Security in the supply chain is an ongoing responsibility. Regular engagement with suppliers is essential to understanding changes, emerging risks and any new dependencies.

What this means for the sector

The Discord incident is just one example, but it reinforces what the dating and discovery industry needs to be aware of. Attackers increasingly target the wider supply chain rather than the platform itself. Sensitive data often sits in external environments, yet accountability ultimately rests with the platform.

As verification and trust-and-safety processes become core components of service delivery, the suppliers behind them must be treated as a key part of their security strategy.

Supply chain security is one of the most important parts of protecting users and preventing incidents that will have a lasting impact on trust, regulation and reputation.