

The GDPR Blind Spot: Sensitive Data Is Protected Inside, Then Exposed in Communication



The GDPR Blind Spot

Sensitive Data Is Protected Inside, Then Exposed in Communication



Oslo, Norway Oct 14, 2026 ([Issuewire.com](https://www.issuewire.com)) - As Norway marks National Security Month this October, Verji Tech warns Nordic organisations that compliance risk increasingly begins when confidential information leaves internal systems.

Nordic municipalities, law firms, audit firms and other organisations handling sensitive information are being urged to reassess a growing GDPR blind spot: **external communication**. While many organisations have invested heavily in securing internal systems, recent regulatory cases across Europe show that data can still be exposed through misdirected messages, collaboration tools and third-party sharing.

This year's National Security Month focuses on digital discernment, highlighting how everyday decisions, from approving access requests to sharing information and responding to messages, can have significant security consequences. Coordinated in Norway by the Norwegian Centre for Information Security ([NorSIS](https://www.norSIS.no)), the campaign reinforces the importance of making informed choices in

an increasingly digital environment.

For organisations handling confidential information, that responsibility extends beyond individual awareness. It also raises an important question about whether sensitive data remains adequately protected when shared outside the organisation.

Norway has already seen enforcement action involving confidential personal information becoming accessible outside intended systems, while European regulators continue to scrutinise cases where sensitive data has been shared with unintended recipients or external parties. For organisations handling **citizen records, identification data, legal documents, financial information and audit evidence**, the compliance question is changing.

It is no longer enough to ask:

“Is our system GDPR-compliant?”

Organisations must also ask:

“Does that compliance continue when the information is shared?”

“The weak point is often not where the data is stored. It is what happens when that data enters a conversation with someone outside the organisation. GDPR responsibility does not disappear when a document is sent,” says **Alf Kenneth Bråthen, CEO & Co-founder, Verji Tech**.

Verji Tech says secure external communication should increasingly be treated as part of an organisation’s GDPR architecture, with stronger control over participants, file sharing, access and visibility once information leaves internal systems.

The issue is particularly relevant to Nordic municipalities and professional services firms, where confidential information moves continuously between employees, citizens, clients, suppliers and advisers.

As National Cybersecurity Month encourages greater digital awareness and more responsible decisions, Verji Tech highlights the need to apply the same thinking to external communication. **Protecting sensitive data should not stop at the boundaries of an organisation’s internal systems.**

About Verji Tech

[Verji Tech](#) is a Norwegian technology company focused on secure digital communication. The Verji platform enables organisations to exchange sensitive information through encrypted communication rooms, secure file sharing and controlled participant access.

Media Contact

TGC Capital Partners

*****@thegatewaycorp.com

<https://www.tgccapitalpartners.com/>

Source : Verji

[See on IssueWire](#)