



# How a Private University Maintains GDPR Compliance by Putting Its Data First

---



Varonis gives us the ability to stop being reactive and start being proactive. We had an external audit this year and we entered it with full confidence. That's not something most universities can say.



## Highlights

### Challenges

- Protecting sensitive data from exposure in compliance with GDPR
- Implementing rapid detection and response techniques to guard against breaches
- Maintaining data security for a remote workforce

### Solution

#### Varonis Data Security Platform:

- **DatAdvantage** gives complete visibility and control over your critical data and IT infrastructure
- **Data Classification Engine** finds and classifies sensitive data automatically
- **Policy Pack** enhances Data Classification Engine with CCPA and GDPR patterns
- **DatAlert** monitors and alerts on abnormal behavior on critical systems
- **Automation Engine** automatically repairs and maintains file system permissions
- **Data Transport Engine** enforces rules for data movement and migration
- **Edge** detects and helps prevent DNS exfiltration attempts

### Results

- Identified key gaps in cybersecurity coverage
- Closed security gaps by adding coverage for VPN, DNS and Azure AD
- Achieved GDPR compliance

## Challenges

### Managing and protecting sensitive data in a complex environment

As one of the longest-established specialist providers of legal education and business training in the UK, the University of Law maintains a sprawling and complex digital environment.

The university has always had to protect sensitive student lifecycle data, financial data, and other sensitive information. CIO Tom Brady has spent years building up a robust defense system to protect this data and mitigate the risk of a breach.



**“Like most universities, our IT security starting point was quite immature. Since then, we’ve built up our resources and governance and introduced a number of market-leading tools. We take cybersecurity very seriously, and adding Varonis was an important addition to our cyber landscape,”**  
**Tom says.**

Two major changes prompted the move to Varonis:

1. The UK’s General Data Protection Regulation (GDPR), which requires businesses to enforce strict data privacy controls, came into effect in 2018.
2. The university’s use of cloud services, especially Microsoft 365, has been steadily increasing—and during COVID-19, it became the new norm.

To achieve GDPR compliance, the university needed complete visibility into on-prem and cloud data stores.

Head of Security Robert Harvey explains:



**“Our base set of tools didn’t give us enough visibility as we started using more OneDrive functionality and moving toward SharePoint and Microsoft 365. We did not know how much data we had or how much of it was stale or classified.”**

Varonis provides the necessary visibility and enables the university to manage and protect sensitive data in their mature, complex environment.



**Robert says, “Varonis helps with visibility. We also gained in-depth security alerting that helps the security team with investigations.”**

**“We’re quite a large university with a lot of data spread out across multiple file servers. We needed help with data analytics and GDPR functions.”**

# Solution

## Industry-leading data protection

With the **Varonis Data Security Platform**, the university knows where their sensitive data exists, who can access it, and what they're doing with it. This allows them to lock down sensitive data and decrease the blast radius of a potential attack.

The university purchased subscriptions for:

- **DatAdvantage for Windows** to gain complete visibility and control over on-prem data stores.
- **Data Classification Engine** to automatically find and classify sensitive data across their environment.
- **Policy Pack** to enhance Data Classification Engine with pre-built CCPA- and GDPR-specific compliance patterns.
- **DatAlert** to monitor and alert on abnormal behavior on critical systems.
- **Automation Engine** to safely and automatically remediate file system permissions en masse.
- **Data Transport Engine** to automatically move, archive, quarantine, or delete data based on content type, age, sensitivity, or access activity.

One year later, the university increased its hybrid defense by adding DatAdvantage modules for **Directory Services**, **OneDrive**, and **SharePoint Online** to their security lineup.



**“The Varonis platform helped a lot during the COVID period. There was a lot of movement on Microsoft Teams at the time and Varonis helped us keep that locked down and monitored while we collaborated in that space,” Robert says.**

## Shoring up their hybrid environment

The following year, Tom and Robert engaged Varonis for a **Cyber Resiliency Assessment**—a simulated attack vs. the university's defenses to measure detection and response capabilities. They didn't want to leave anything to chance.

During the simulation, multiple attack vectors were tested to check the resilience of the system. They performed eight test cases, including a simulated ransomware attack.

The pre-Varonis tech stack successfully detected four test cases out of eight, but the other four slipped by undetected. Only Varonis caught and helped prevent the simulated ransomware during the encryption process.

The simulation also revealed a large security gap: a lack of insight into DNS, VPN, and web proxies resulted in an undetected breach. The risk was compounded by the high traffic volume on the university's VPN.

To fill this security gap and better protect students and staff while they work remotely, the University of Law purchased **DatAdvantage for Azure** and **Edge**.

“

Tom says, “Varonis is such an important part of our IT security landscape. Now we’re not afraid to test our defenses and we’re pushing boundaries to see if we can highlight anything that’s missing. That’s a totally different mindset compared to where we came from.”

**“Varonis provides full-picture visibility of where our data is across all of our different platforms. From a security aspect, it’s really useful to have that extra level of alerting and monitoring especially on our sensitive data.”**

# Results

## Security gaps filled with Varonis monitoring and alerting

The University of Law uses Varonis to monitor over 5 TB of data (almost 3 million files) across all of its data sources, including thousands of SharePoint and OneDrive sites, hundreds of Microsoft Teams sites, and numerous private channels.

Having this visibility is proving crucial as the university strives to maintain compliance.



**Robert says, “Varonis saves quite a lot of time. Investigations that used to take half a day are now done within minutes in some cases.”**

By arming the security team with deeper insights into their environment, the Varonis Data Security Platform:

- Enables the University of Law to classify data stored on prem and on the cloud, restrict access to sensitive data, and enforce healthy data retention policies.
- Empowers the maturation of the university’s threat detection and response procedures.
- Provides the visibility and control that the security team needs to maintain compliance with GDPR.


As for the next steps, Tom and Robert are gearing up to demo **DatAdvantage Cloud** to probe for blind spots and see if they can tighten up their cloud security even further.



**“I would recommend taking the same journey that we went on: Put in the core functionality. Make sure it’s doing what’s expected. Reap the results of that. Then build upon it from there,” Tom says.**



**“Adding in modules over time has really expanded our capabilities,” Robert adds. “It’s been easy to slot the next module in, and everything comes together to enrich your reports and enhance the data you can see.”**



**“Varonis is such an important part of our IT security landscape. We’re not afraid to test our defenses and now we’re pushing boundaries to see if we can highlight anything that’s missing. That’s a totally different mindset compared to where we came from.”**



# Put your data first with Varonis.

Find and solve your biggest security gaps to mitigate risk.

[Request a demo](#)