WHITE PAPER (Titus)

Works Councils: How to Balance Data Protection with Worker Privacy

The Data Protection & Privacy Challenge

No matter what industry you are in, protecting data is a top priority. To protect data, many organisations implement systems which monitor all internet traffic in order to catch inappropriate data sharing. However, not all correspondence that originates at the office is business related. While they may be at work, employees are still entitled to manage their personal affairs and build relationships in private without being subject to employer surveillance.

In particular, European government and workers' rights advocates have established rules and guidelines for the protection of worker privacy, most notably with the European Works Councils Directive 94/45/EC, and the proposals in the Article 29 Working Party's "Working Document on Surveillance and Monitoring of Electronic Communications in the Workplace." It is their view that using a security system which remains in constant surveillance mode to scan all employee correspondence is a violation of a worker's privacy. Indeed, if any violations are found via these means, it is very probable that they would not be admissible as legitimate grounds for employee discipline.

While it would be considered acceptable in most jurisdictions to monitor and review high level, aggregate, and anonymized data, any continuous blanket content monitoring would not be considered fair, proportionate or necessary. Therefore, using security technologies which have no ability to discern personal from business correspondence without first examining the data's content is not a solution.

So, how can an organisation strike the right balance between the need to protect business data and the rights of the workers to personal privacy? The answer is information classification.

WHAT IS A WORKS COUNCIL?

A 'works council' is a group of elected employees whose mandate it is to protect employee interests within the workplace. Works councils must be notified in a timely manner of any projects which impact the employees, such as changing work methods, implementing new technologies, or changes to data processing. In some countries, the works council's approval may be necessary before the employer can begin the project.

Works councils are not trade unions. However, individual elected members on the works council may be affiliated with a union.

Classify as Private

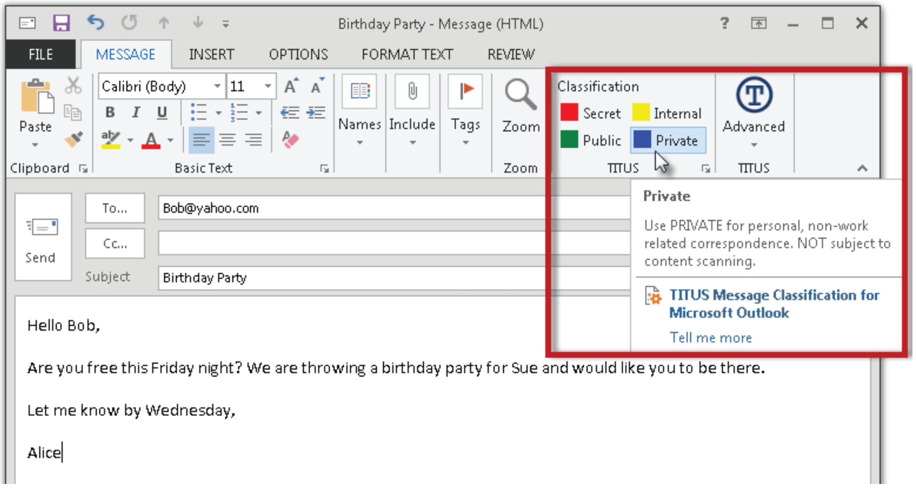
The difficulty that gateway data loss prevention (DLP) systems face, in regards to worker privacy, is that they must scan the contents of the data in order to identify it. Without data identification, it is not possible for the system to know which policy to apply to the data. Titus Classification solutions enable workers to identify the data they create. Titus' easy to use interface guides workers in the application of proper classifications without the need for automated content review. Once the classification is attached to the data, whether it be a document, image or email, both electronic gateway systems and other employees will be aware of the data's sensitivity and how it should be secured.

In order to protect worker privacy, Titus Classification solutions can be configured with a special classification for employees' personal documents and email. An "Employee Private" or simply "Private" classification will instruct content scanning systems to ignore files where the "Private" classification is used, thereby making it possible to maintain data security without violating privacy regulations.

The Article 29 Working Party has set guidelines that organisations should keep in mind when engaging in network monitoring activities.

1. Are Workers Aware of the Monitoring Activity and Policy?

Titus understands that the people who create and use data are best at determining the classification since they know the content and understand the context. The Titus interface is user friendly and designed to easily guide employees in making the correct classification choice. The classification dialogue can be customised with tooltips and help options that provide specific policy information for each classification, and the consequences when it is used. The information displayed for the "Employee Private" classification would clearly indicate that these documents and emails should not be subject to content scanning.



To... Bob@yahoo.com

Subject Birthday Party

Hello Bob,

Are you free this Friday night? We are throwing a birthday party for Sue and would like you to be there.

Let me know by Wednesday,

Alice

Private

Use PRIVATE for personal, non-work related correspondence. NOT subject to content scanning.

TITUS Message Classification for Microsoft Outlook

Tell me more

Figure 1 – One Click Classification "Private" showing tool tip.

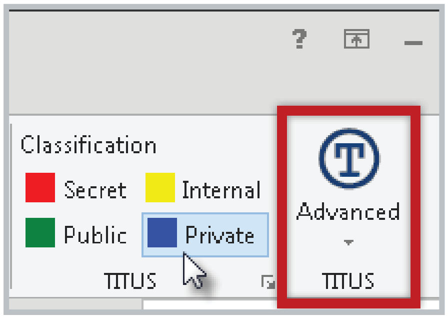
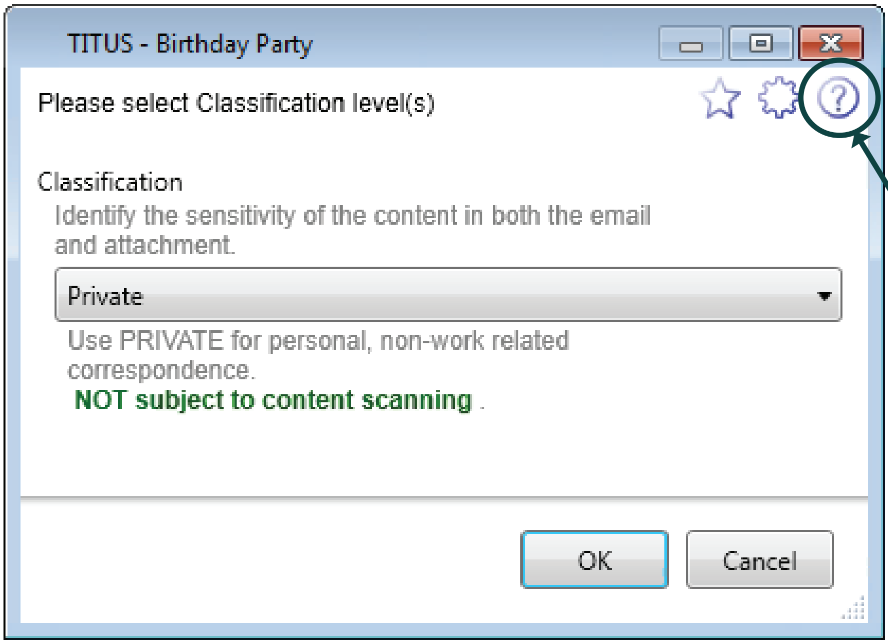


Figure 2 - Advanced classification button opens the classification dialogue.



Please select Classification level(s)

Classification

Identify the sensitivity of the content in both the email and attachment.

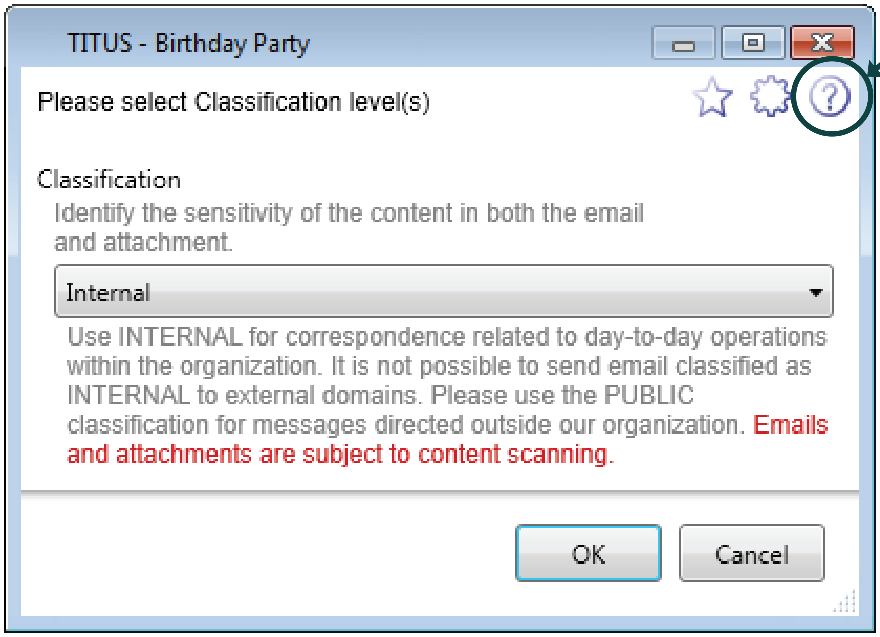
Private

Use PRIVATE for personal, non-work related correspondence.

NOT subject to content scanning .

Figure 3 – Full classification dialogue showing full field descriptions.

QUICK ACCESS TO MORE DETAILED POLICY INFORMATION AND HELP.



Please select Classification level(s)

Classification

Identify the sensitivity of the content in both the email and attachment.

Internal

Use INTERNAL for correspondence related to day-to-day operations within the organization. It is not possible to send email classified as INTERNAL to external domains. Please use the PUBLIC classification for messages directed outside our organization. Emails and attachments are subject to content scanning.

Figure 4 - Classification field descriptions customizable for each classification value.

2. Is it Necessary?

Titus understands that the people who create and use data are best at determining the classification since they know the content and understand the context

3. Is the Proposed Processing of Personal Data Fair to the Workers?

No document or email content can be scanned without the workers' consent. By giving all employees clear instructions and the ability to choose the classification, they are empowered to opt into or opt out of automated scanning of the content they create and send.

4. Is it Proportionate to the Concerns it Tries to Ally?

Organisations must trust that their workers are behaving ethically. TITUS Classification is a constant reminder and guide for users, helping them to comply with security policy. TITUS Classification also makes it possible for organisations to scan only business files and correspondence to verify data security policies are being respected.

There may be times, however, when an employee is suspected of abusing their private email classification to send sensitive data. It should be noted that by applying classification to documents and email it is possible to gather a different high-level and anonymous data set by tracking volume of email by classification. If an organisation has legitimate and justifiable concern that a specific employee is engaging in harmful activities, the investigators could start by checking for changes in her/his "Private" email traffic without peering into the content of the messages. As legal justification is collected using these non-invasive techniques, more invasive tactics, such as secret content scanning, could then be considered.

5. Is the Data Collected Used Only for the Legitimate Purpose Specified?

Using a "Private" classification ensures that personal worker data will remain anonymous and will not be collected. Since no personal information is being collected on a day-to-day basis, questions around how the data is used, how long it is kept, and if it is copied are not relevant.

Benefits of Titus Classification

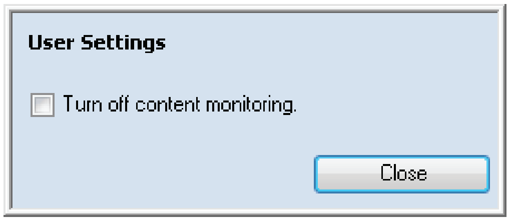
While it may make some organisations, particularly those headquartered in North America, uneasy to allow their workers the option to save and send documents or emails without content scanning, Titus customers have found that their employees do wish to maintain a secure working environment. When workers are consulted regarding security policy and made aware of the shared consequences if the organisation is compromised, overall data protection improves. Workers that create or manage sensitive data are more likely to feel a level of ownership and will therefore classify the files appropriately. In addition, because Titus enables users to classify documents with just one click, adding classification is not seen as a hindrance to productivity.

When documents and files are classified, the Titus Classification software can—without scanning content—compare the attachment classification with the outgoing email classification. If an email is marked "Private" but the attachment is not, Titus Classification can stop the email from being sent in order to prevent improper distribution. A pop-up will notify the worker as to why the email was blocked and provide options to correct the discrepancy, such as: removing the attachment, changing the email classification, or suggesting the worker request a classification downgrade for the document from a manager (Titus Classification solutions can be configured to restrict classification downgrades to specific workers).

In addition to using classification schemes to control policy around content scanning, Titus also allows administrators to set up a policy opt-in/opt-out control for users. At the most basic level, using the opt-in/opt-out toggle to turn off content monitoring would prevent Titus from examining that user's data, regardless of the classification. Yet, the opt-in/opt-out toggle does not have to be quite so blunt; administrators can customise exactly how the opt-in/opt-out toggle affects policy.

For example, an organisation may have a business unit that deals with highly sensitive information, such as personnel files. Because a personnel document leak from the HR department could be exceptionally damaging, Titus can be configured in such a way that the "Private" classification applied to an email specifically by Human Resources (HR) workers prevents content analysis of the email only. In this case, attachment contents will be scanned despite the "Private" email classification. However, Human Resources workers could still be afforded the option to completely shut off attachment surveillance on email classified as "Private" using the opt-out toggle. As a customizable tool, the opt-in/opt-out policy toggle can provide added nuance to worker privacy that is not otherwise afforded in regular, day-to-day operations.

Figure 5 - Opt-in/opt-out toggle



User Settings

□ Turn off content monitoring.

Classify to Protect Data and Workers' Rights

Worker privacy is a serious issue. Finding a balance between the workers' right to private communication and the need to protect sensitive data can be difficult to achieve if the security systems in place do not know how to properly handle unstructured information. However, Article 29 Working Party recommendations can be respected and implemented successfully using Titus Classification. Titus policy reminders ensure that workers are consistently and accurately informed of the policies that apply to their specific context, be it their local region or department. Informed workers can confidently choose the appropriate classification and apply policy with a single click. Titus can also provide immediate feedback and remediation options to users should it detect policy violations, such as a discrepancy between the document and email classifications. Most crucially, Titus applies the classification as persistent metadata which other security technologies, including content surveillance systems, can use to enforce privacy compliant handling instructions.

With Titus Classification you can be confident that both your data and your workers' rights are being protected. For more information about how Titus can help your organisation identify, protect and confidently share your sensitive data, please visit: www.titus.com

Benefits of Titus Classification

- Comply with worker privacy laws
- Workers provided choice; opt-in to content scanning
- Easy to use; high user acceptance
- Accurately restrict content monitoring to work-related data
- Remind and guide workers through data security policy
- Target classification options, language and policy to different work groups
- Avoid unnecessary monitoring
- Classification informs downstream security technologies (DLP, RMS, etc.)
- Catch and correct policy violations before they happen
- Customise/limit data captured in the audit logs
- Additional detail (classification) for high level, anonymized monitoring

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.