WHITE PAPER

proofpoint.

DATA PRIVACY IN YOUR OWN BACKYARD

STAYING SECURE UNDER NEW GDPR EMPLOYEE INTERNET MONITORING RULES

TABLE OF CONTENTS

INTRODUCTION

To date, General Data Protection Regulation (GDPR) compliance efforts have focused mostly on protecting customer data. But security teams must also consider how the new rules affect the data they collect from their own employees.

Many organizations monitor, log and report on workers' digital communications. This effort often includes internet usage. It's easy to see why. The web and personal email services are a major source of security threats.

Under the GDPR, they're also a potential privacy minefield. Without the right tools and approach, the rules could constrain these efforts and hurt your security posture.

This paper summarizes key mandates of the GDPR when it comes to employees' personal internet use. It also explains how to stay secure without running afoul of the law.

KEY GDPR PROVISIONS

GDPR replaces the 22-year-old EU Data Protection Directive. At its core, the GDPR aims to put EU residents in control of their personal data. It regulates how their data is:

- Collected
- Processed
- Stored
- Deleted
- Transferred
- Used

No matter where it is based, any company that does business in Europe or handles the personal data of EU residents must follow the new rules.

Developing GDPR compliance plan is critical. Failing to comply could lead to hefty fines—up to 4% of annual global revenue or €20 million whichever is higher. This amount is far higher than any fines that individual EU countries can impose today.

GDPR AND EMPLOYEE PRIVACY: ARE YOU COMPLIANT?

GDPR rules also apply to your employees' privacy in the workplace. Many security programs monitor employee activity on the network, company-owned devices and cloud services. Under GDPR rules, they may become tricky balancing acts for security teams.

Under the GDPR, you must weigh your security needs against workers' right to privacy. Sometimes security needs win out, limiting employees' right to privacy. But even then, your response must be "proportional."

A monitor-everything approach might seem convenient. But convenience alone would not warrant invading employees' privacy.

GDPR GUIDANCE

EU rules governing how you can monitor email and web stem from these edicts:

- European Convention on Human Rights. Articles 8 and 10 outline a right to privacy and freedom of expression.
- EU Data Protection Directive. The directive guides EU member states to regulate how personal data is processed. It took effect in 1998.
- Article 29 Working Party working documents. Relevant guides include "Processing of Personal Data in the Employment Context "(2001) and "Surveillance & Monitoring of Electronic Communications in the Workplace" (2002).

NO MATTER WHERE IT IS BASED, ANY COMPANY THAT DOES BUSINESS IN EUROPE OR HANDLES THE PERSONAL DATA OF EU RESIDENTS MUST FOLLOW THE NEW RULES.

LEGAL PRECEDENT

Case law stemming from the Convention on Human Rights illustrates three principles:

- Workers have a rightful expectation of privacy at the workplace—even if they use an employer-owned device.
- The general principle of secrecy of correspondence covers communications at the workplace. This likely includes email and file attachments.
- Respect for private life includes, to a certain degree, the right to form and nurture relationships with other people. Some of these relationships take place at the workplace. This reality limits employers' surveillance prerogatives.

[1] Oracle. "Accelerate Your Response to the EU General Data Protection Regulation (GDPR)." January 2017.

WATCHING THE WATCHERS: KEY PRINCIPLES OF EMPLOYEE MONITORING AND PRIVACY

The clearest guidance on how organisations can monitor employee communication comes from the Article 29 Working Party. The EU advisory board includes the data protection authority of each EU country, the European Data Protection Supervisor, and the European Commission.

The group has provided some guidance through these documents:

- "Working Document on the surveillance of electronic communications in the workplace (WP 55)"
- "Opinion 8/2001 on the processing of personal data in the employment context (WP 48)"
- "Opinion 2/2017 on data processing at work (WP 249)," which complements the previous two documents

Here are some highlights.

A BAN ON PERSONAL WEB USE IS UNREALISTIC

"A blanket ban on personal use of the Internet by employees may be considered to be impractical and slightly unrealistic." (WP 55)

"…[A] blanket ban on communication for personal reasons is impractical and enforcement may require a level of monitoring that may be disproportionate." (WP 249)

MONITORING MUST BE NECESSARY

"It would only be in exceptional circumstances that the monitoring of a workers mail or Internet use would be considered necessary" (WP 55)

"The legitimate interest of employers can sometimes be invoked as a legal ground, but only if the processing is strictly necessary for a legitimate purpose and the processing complies with the principles of proportionality and subsidiarity." (WP 249)

IF NECESSARY, IT SHOULD BE MINIMIZED

"To the extent reasonably possible Internet policy should rely on technical means to restrict access rather than on monitoring behaviour." (WP 55)

"Employers must take the principle of data minimisation into account when deciding on the deployment of new technologies. The information should be stored for the minimum amount of time needed with a retention period specified. Whenever information is no longer needed it should be deleted." (WP 249)

IT MUST BE TRANSPARENT

"Workers need to be informed about the systems implemented both to prevent access to certain sites and to detect misuse" (WP 55)

"Effective communication should be provided to employees concerning any monitoring that takes place, the purposes for this monitoring and the circumstances, as well as possibilities for employees to prevent their data being captured by monitoring technologies. Policies and rules concerning legitimate monitoring must be clear and readily accessible." (WP 249)

YOU CAN'T USE EMPLOYEE CONSENT TO OVERRIDE PRIVACY RIGHTS

"…[I]t is misleading if it (Employer) seeks to legitimise… through consent. Reliance on consent should be confined to cases where the worker has a genuine free choice…" (WP 55)

"Employees are almost never in a position to freely give, refuse or revoke consent, given the dependency that results from the employer/employee relationship. Given the imbalance of power, employees can only give free consent in exceptional circumstances, when no consequences at all are connected to acceptance or rejection of an offer." (WP 249)

THE RULES APPLY TO CLOUD SERVICES

"Where employees are expected to use online applications which process personal data (such as online office applications), employers should consider enabling employees to designate certain private spaces to which the employer may not gain access under any circumstances, such as a private mail or document folder." (WP 249)

FINDING THE RIGHT BALANCE

Figure 1 highlights the challenge. You must follow GDPR rules. But you also want to minimize threats stemming from workers' personal activity.

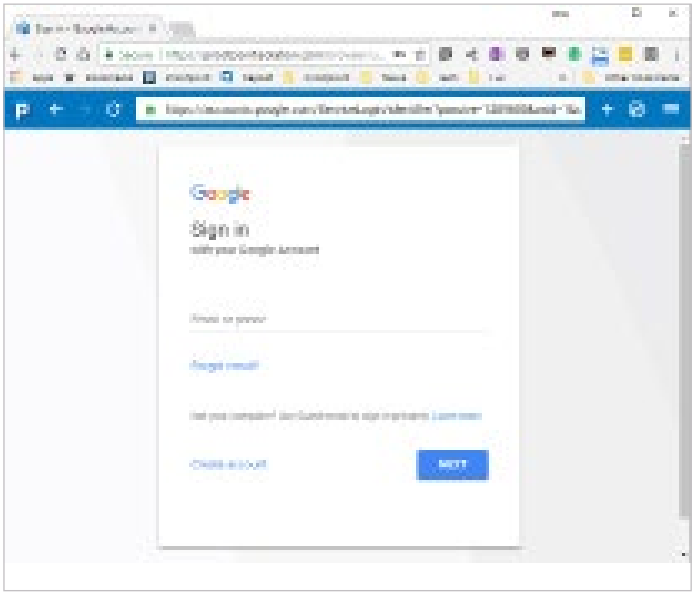
Figure 1: Balancing security and employee privacy

THE POWER OF ISOLATED BROWSING

Fortunately, you don't have to sacrifice one for the other. Web isolation—separating workers' personal web traffic from your corporate web traffic—solves both issues.

Proofpoint TAP Isolation allows employees to browse freely and privately in a separate, protected session. It encompasses the same intelligence from our Targeted Attack Protection (TAP) suite of security products. The broader TAP suite stops advanced threats through email, the web, the cloud, and mobile devices.

With TAP Isolation, users browse the web as normal. We isolate their activity in a secure, remote container that defends users from high-risk content they may run into while browsing. Users don't notice any difference, and they don't need to install anything. But any unsafe code they encounter stays out of their endpoints and your environment.



TAP Isolation separates personal web browsing, including web-based email, from the corporate network.

This split stops threats stemming from personal internet use. And by stopping corporate and personal activity from comingling on users' devices, TAP Isolation also prevents many compliance issues beyond GDPR.

HOW IT HELPS ORGANIZATIONS

TAP Isolation protects organizations and their staff by separating corporate and personal web browsing.

It creates an “air gap” between business and personal networks, sharply reducing malware, data loss and compliance risks. And by allowing employees to browse privately, it fully complies with GDPR privacy rules.

With TAP Isolation, you can restrict access to unsafe websites on your corporate network without having to monitor or block personal web browsing.

HOW IT HELPS EMPLOYEES

With TAP Isolation, your people get direct, safe and unmonitored access to the web. Their browsing sessions are secure and encrypted no matter where they’re connecting from. They can access websites even if those sites are blocked on the regular corporate network. And they get the peace of mind that comes with knowing:

- Their personal information will remain private and cannot be monitored
- Their web activity won’t inadvertently harm the organization

CONCLUSION

GDPR’s protection of personal information goes beyond customer data. It directly applies your employees, contractors and vendors. In much the same way it guards consumers’ privacy, GDPR protects workers’ personal activity—even on your network and devices.

Security teams must accommodate workers’ right to a private life in the workplace. They must also safeguard the enterprise. TAP Isolation helps ensure that your security programs do both.

LEARN MORE

To learn more about how TAP Isolation can help you balance security and employee privacy, visit proofpoint.com/us/products/targeted-attack-protection-personal-webmail-defense

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.