Issues in Employee Privacy

An employee privacy policy is documentation specifying an organization's rules and procedures for gathering, using and disclosing the personal information of former, current or prospective employees. Some elements of privacy policies may be mandated by labor laws, while others are specific to a given organization.

An employee privacy policy should define what constitutes personal information and the means by which it might be collected. As a rule, most companies define personal information to include all employee data (such as home address and work history), and all communications that are not work-related.

A policy should clearly stipulate situations in which an employee should not assume their data and communications are private. Phone calls, texts, emails and social media communications that are transmitted on corporate-owned equipment, for example, are not legally protected. Software and websites those are not required for business purposes may be restricted according to policy or blocked to prevent problems.

It's also important to specify under what conditions employee data will be disclosed. Those conditions could include situations where the employee had consented, emergency situations and legal situations, such as a warrant or a court order.

Privacy policies should also disclose any employee monitoring systems, such as video recording. Employees should be provided with copies of the privacy policy and should be required to confirm that they have read and understood it.

Personal data is becoming more valuable as networked devices are frequently used for work and personal purposes. With sensitive data exchanged on these devices, concerns about personal data tend to exist -- with employees concerned that their data may be poorly handled and leaked to malicious entities. A good employee privacy policy aims to prevent these concerns with upfront disclosures.

Frequent employee privacy concerns

Privacy-related issues employees are likely to be concerned include the following:

- What personal information/data is being collected about them.
- Why it is being collected.
- With whom it is being shared.
- How their sensitive personal information/data is being protected.
- Email privacy.
- Whether use of company assets (such as mobile devices, internet) is being monitored.
- Whether they are subject to video surveillance.
- Whether they must submit to background checks and/or drug tests.
- Whether their use of social media outside the company is being monitored and/or can be controlled.
- What happens to their personal information/data after they are terminated and/or no longer working for an employer.
- What their privacy rights are in relation to their personal information/data, such as their ability to access, refuse to provide, request deletion, amend, correct or transfer their personal data.

Building an employee privacy policy

In general, a great way to prepare for creating an employee privacy notice is to create a personal data processing register, data inventory and/or data map, which identifies the following:

- Business processes that your organization performs involving personal data and their purposes.
- How the data is collected for each business process.
- How the data is used by the organization.
- Where the data is stored and who (internally and externally) it is shared with.
- Where and how data is transferred.
- How data is protected.
- How long data is retained.

The above information can then be used to determine what privacy regulations apply to the personal information/data, and can be used to create compliant processes and a privacy notice, which addresses the requirements of those regulations.