HAVE YOU THOUGHT ABOUT YOUR AUDIT LOGS WHEN COMPLYING WITH POPIA?

Category: Privacy Law and POPIA,Privacy Law, Infosec, and POPIA
written by Lucinda Botes | April 5, 2024

Logs! Audit logs, system logs and error logs are often a neglected business process when organisations consider their data privacy compliance.

Audit logs by itself are generally not expressly listed as a category of personal information under data privacy laws. Logs are records of actions or events of internal activity that is done on a system. Logs may contain details such as a user’s identity, IP address and timestamps.

Even though logs are not inherently considered to be personal information, audit logs may contain information which depending on the context are able to identify a particular individual. For example, if an audit log, associated with my employee number that is linked to a static IP address, captures that I accessed the company’s payroll system to view my December payslip at 08h00 on Thursday, 2 April 2024, it is clear to see that the audit log is personal information.

This means that audit logs, to the extent that they personal information, should be treated in accordance with applicable data privacy laws.

Organisations should therefore apply the following:

- As far as possible, organisations should minimise the inclusion of personal information in audit logs whenever possible. Only information necessary for security and compliance purposes and avoid logging sensitive information such as identity numbers or passwords.

- Apply pseudonymisation, anonymisation or data masking techniques to data in audit logs to reduce the risk of unauthorised access or exposure.

- Encrypting data both in transit and at rest to protect it from interception as well using strong encryption methods ensure that encryption keys are securely managed and rotated regularly.

- Implementing access controls to restrict access to audit logs to persons who need to know it.

- Ensuring that logs containing personal information are only retained for the minimum period based on regulatory requirements and business need. Further ensuring that obsolete log data is deleted on a regular basis.

- It is further helpful to develop logging policies and procedures outlining the guidelines for audit log creation, management, and review. Ensure that personnel responsible for managing audit logs are trained on these policies and follow them consistently.

- Ensuring that it notifies data subjects of how it processes audit logs through privacy notices.

- If your organisation records a large number of logs, it is important that it is included in regular privacy audits and reviews to verify compliance with privacy requirements and identify any gaps or issues that need to be addressed.

- If organisations use a third-party logging service and solutions, it is important that the organisation ensures that the service provider is able to demonstrate privacy compliance through data processing agreements and security measures to confirm that audit log data is adequately protected.

By implementing these measures, organisations can enhance the privacy compliance of their audit logs, mitigate the risk of unauthorised access or exposure of sensitive information, and demonstrate their commitment to protecting individuals’ privacy rights.

Contact us for more good, clear, precise advice.