

ISO 27018 PERSONALLY IDENTIFIABLE INFORMATION

Provide your cloud services customers with transparency on how responsibly you manage personally identifiable information

BUSINESS CHALLENGE

The volume of cloud managed information continues to grow, and as public breaches are coming to light and new legislation is being brought in, customer awareness is focused on the risks of their sensitive information being abused.

WHAT IS ISO 27018?

The international code of practice for the protection of Personally Identifiable Information (PII) in public clouds acting as PII processors builds upon the best practice controls laid out in ISO 27002 and establishes some new controls for cloud data privacy. They include the separation of the development, testing and operational environments when personal data is used for testing, information backup management dealing with multiple copies of data, its recovery and erasure and providing information about this to the customer, event logging, their review, recording changes in the privacy of information and customer disclosure regarding this. Further guidance in the annex includes: customer access rights, appropriate use of data, deletion of temporary data, subcontractor use and confidentiality agreements for those conducting PII processing, document management, a policy for PII return, transfer, restoration and disposal, physical media movement authorization, restriction on non-encrypted media use, and mandatory encryption when using public networks, destruction of printed PII, use of unique IDs for cloud customers, user access logging, disabling expired user IDs, contractual coverage of minimum security controls with customers and subcontractors, disclosure of the countries where PII will be stored and ensuring PII reaches its destination.



WHO IS ISO 27018 FOR?

Those cloud services providers that process significant volumes of PII will be able to seek certification to ISO 27001, ISO 27017 and ISO 27018 or a combination of these standards to provide transparency to their customers about the responsible management of their clients' sensitive personal data.

For more information:
certification.contact@bureauveritas.com
www.certification.bureauveritas.com



BUREAU
VERITAS

Shaping a World of Trust