Data Handling and Security

Frequently asked questions

Where does my data reside?
Data uploaded to Connect will temporarily be located on PwC Servers in the US. These servers are under the jurisdiction of PwC Global IT, an independent entity operated in the UK. Once received, data will be imported to PwC Cloud Servers residing in Canada where all validation, analysis and review will occur. Data temporarily residing on the PwC Servers in the US will then be deleted.

What data handling procedures are in place?
Proactive data management and protection plays an important role in upholding our brand reputation and building trust with our clients and broader society.

Our global network has developed the Network Data Protection Program (NDPP), which serves as a common set of standards across the network to address matters of data governance, protection and appropriate use of personal data from our people, clients, vendors and other stakeholders. The NDPP also meets the requirements of the European Union's General Data Protection Regulation (GDPR), which came into effect on May 25, 2018.

How does PwC keep data secure?
Data must be stored in a secure environment keeping in mind the sensitivity and confidentiality of the information. Additionally, we ensure appropriate protection is in place when handling classified information. Our partners, principals and staff follow IT security policies and guidelines that communicate individual responsibility for safeguarding IT resources.

How long does PwC store my data?
Data must be stored only as long as it is necessary to do so. Once the data is no longer required, it is destroyed.

Will my data be housed in the cloud?
PwC infrastructure is built on a Hybrid Cloud Services (HyCS) hosted in Microsoft Azure which is fully managed by PwC local and Global IT services. Azure SQL data is secured by a number of built in measures including SQL Always Encrypted and Azure SQL Database Auditing. Additionally, system controls are applied at an enterprise level to all on-site and cloud based server environments.

What are the extra measures that PwC takes to ensure data security?
We apply baseline controls at the server level, which is similar to endpoint security controls. These controls include:

- Maintaining the latest version and patch levels of operating systems and software.
- Privileged access to the operating system is restricted and monitored using Enterprise Privileged Access Management Vault technology.
- Anti-malware software is installed, centrally maintained and updated.
- Advanced Threat Prevention and Detection software is installed and centrally maintained.
- Enterprise Gateway Data Loss Prevention and Web Proxy software is centrally installed and actively restricts and monitors use of external storage services and websites based on policies.

Summary of PIA Assessment on the entire analytics infrastructure hosted by PwC:

Based on the Privacy Impact Assessment conducted, the Privacy Officer concluded that there was minimal risk in adopting the new Electronic Trust Transfer Review (ETTR) project. Minimal risk in this context refers to risk to the security of audit information. This includes factors such as where the information is stored, who has access to the information, and the security in place for our information if it is stored by a third party.

The Privacy Officer deemed that although the information is stored on PWC Connect servers, there are substantial security measures in place to protect audit information. Similarly, the contractors involved in the ETTR program from PWC have taken LSA Privacy training and have agreed to safeguard the confidentiality of audit and analytics information.

Data Security

PwC has thorough system security and data handling procedures designed to prevent unauthorized access to client confidential information, including unauthorized access by government entities. Their staff and contractors are regularly trained on these procedures to ensure these procedures are adhered to at all levels. Unauthorized breach of data is reported, investigated and corrective actions are taken. In addition unauthorized access affecting data held on behalf of LSA and its members will be reported to LSA