GDPR

General Data Protection Regulation

In effect as of May, 2018

Statement of Compliance
General Data Protection Regulation (GDPR)

What is the GDPR?
The General Data Protection Regulation (GDPR) is the new European legislative framework regarding the processing and movement of personal data, which businesses use to support their service and product offers. This Regulation covers all the residents of the European Union. It requires that those responsible for data processing as well as any subcontractors take technical and corporate measures to guarantee the security of personal data during processing.

What is the goal of the GDPR?
The goal of the GDPR is to become the European Union's new legislative reference regarding the protection of personal data, thus replacing a guideline dating back to 1995. It was necessary to reform the outdated European legislation in light of the expansion of the digital economy, the emergence of new uses and the establishment of new business models.

When did the GDPR come into effect?
The GDPR came into effect on May 25, 2018.

What is personal data?
Personal data is information by which an individual can be identified, directly or indirectly. Such information includes the following: name, photo, IP address, phone number, login credentials, mailing address, fingerprint, voice recording, social security number, email address, etc.

Some data is sensitive as it contains information that can give rise to discrimination or prejudice:
Political views, religious beliefs, union involvement, ethnicity, sexual orientation, medical condition and philosophical ideas are sensitive data. Such data is subject to a specific framework which prohibits any gathering without prior clear, explicit and written consent.

To whom does the GDPR apply?
Be it a business, a subcontractor or an association, any entity handling personal data about Europeans must comply with the GDPR. Important note: The Regulation is not bound by the European territory. Canadian, Japanese or Chinese groups that collect and process personal data must also comply with the Regulation.

IT Cloud and the GDPR
Our organization follows the Policy on Information Technology Security. IT Cloud therefore maintains a high level of security in its daily operations and engages in ongoing assessment, risk management and enhancement processes.

Our organization has mapped the full range of data processing procedures involved in our operations. This processing structure allows us to identify the processes involving personal data and to orchestrate data protection throughout the gathering, hosting and processing of data, and upon development of new applications or services.

Such protection measures can be of the following types:

- Material (firewall, proxy, closed network, regular renewal of work stations and servers, etc.).
- Methodological (various security levels and tests during development phases, monitoring tools, daily and incremental backups, SSL/HTTPS protocols for our tools);
- Software-based (antivirus software, regular software licence updates and renewals, secure tools and modules).

Our data centres are in full compliance with industry standards. We use cryptography for server connections as well as for document transfers, including Secure Sockets Layer (SSL) technology. Our data centres feature access control systems. These systems allow only authorized staff to access restricted areas. Equipment is kept in secure rooms designed to prevent unauthorized intrusions and to resist variable climate conditions. Presence detectors are also in place inside the centres to prevent unwanted intrusions.

We are committed to working only with instances who use equal security measures and whose operations comply with the GDPR.

Where do we keep service-related personal data?
The personal data related to our backup services is hosted on IT Cloud servers located in our Canadian data centres.

Personal data related to services hosted by third parties is located in Canada and France. IT Cloud cannot be held liable for data processing by such third parties.

Transparency

All of our employees have undergone a criminal background check and have entered into a confidentiality and non-disclosure agreement. They have been trained in data protection. Only authorized individuals have access to the servers and such access is subject to restrictions and limited rights.

Each client has a unique username and password.

Data retention timeframe

Upon request, we will delete your data, including in the event of a breach of contract or migration to or from a competitor, within 15 days.

Only the data required for tax or legal purposes will be kept.

Shared responsibilities

This Statement of Compliance, issued as a subcontractor, does not exempt our final clients from the obligation to comply with the GDPR and to control the number of persons accessing our tools, to properly use strong passwords, to implement the necessary physical and software safeguards to secure the incoming or outgoing data, to be forthcoming about the origin of the gathered data, to refrain from using our tools in an abusive manner for reprehensible operations, and to follow our ethical and technological recommendations.

For information about our compliance with the Regulation and data processing, write to us at privacy@itcloud.ca