Articque measures under GDPR regulation C&D Online Cloud

Information on the C&D Online Cloud Server hosting and its administrators:

- Cloud provider company is Castle IT company located in Saint Avertin – France
- C&D Online Cloud Server is located in Larcay - France
- Server administrators are Articque staff only, located in Fondettes - France.

Implemented actions on the C&D Online Cloud server:

- Firewalls have proper configuration and are regularly updated.
- We have a user access control management policy.
- Network administrator privileges are only used when needed.
- Network administrator has a separate account from his user account.
- Unique passwords of sufficient complexity and regular renewal (but not too frequent - 6 months) on all devices for Articque administrators and employees.
- Regular renewal of user's passwords (every 6 months and inability to reuse old passwords).
- Regular software updates, by using patch management software.
- Final user can delete their own data at any time and deletion at the end of the contract is mandatory.
- Regular secure decommissioning and wiping (that renders data unrecoverable) of old software and hardware at suitable moments.
- Real-time anti-virus, anti-malware and anti-spyware protection.
- Administration tasks can only be performed from local network or via VPN access.
- Encryption of client data on the servers.
- Implementation of secure configuration on all devices (including smartphones).
- Prevention systems.
- Regular intrusion detection tests to increase security level.
- Data backup is scheduled and checked every working day.
- Wi-Fi passcode are kept confidential and changed regularly.
- Wi-Fi access to the corporate network uses WPA2-TKIP.

Organizational measures implemented by ARTICQUE:

- Non-disclosure measures are applied each time client data are processed (demo, formation…) with data deletion once the process is completed.
- Access and processing of personal or sensitive data is strictly forbidden.

Cartes et Données Desktop and Articque Platform are the only suitable solutions to the processing of personal or sensitive data. The C&D Online Cloud is not suitable for this task. (cf. Art 12.7 of C&D Online Cloud terms of sales)

- Training sessions are provided to the staff about obligations regarding data processing, security weakness identification and risk prevention.
- All administrative documents (contracts, bills…) are stored in secured cabinets.
- Printing of sensitive documents by the Articque staff is not allowed.
- Use of personal hardware or software in workplace context is not allowed.
- Use of a personal email account for business purposes is not allowed.

Good practices to be applied to geocoding by THE CUSTOMER:

Users must not user first name or last name associated with postal addresses (anonymization). We advise to use an id instead of first and last name (which will afterward allow them to link it to real data), and to maximize the simplification of the files they send by only including the fields that are required to perform the geocoding operations or drawing, in accordance with article 4 of GDPR, which defines pseudonymisation.

Legal referent contact:

Aurélie JOUBERT – Legal Consultant
ajoubert@articque.com

Corporate security policy referent contact:

Josip DUPUIT – IT Manager
jdupuit@articque.com