Articque measures for C&D Online under GDPR

Articque measures for C&D Online under GDPR - version 8.1		
Writing	T. Laugier	17th march 2023
Validation	J. Dupuit	17th march 2023
Approval	H. Auguet / A. Joubert	20th march 2023

Information about the C&D Online server hosting and its administrators:

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

Actions implemented on the C&D Online server:

- Firewalls have proper configuration and are regularly updated.
- We have a user access control management policy.
- The server's administrator accounts are local and dedicated to this server.
- Access to the server's administrator account is restricted to authorized persons only.
- Administrator accounts password are renewed every 6 months.
- C&D Online account passwords are subject to the following requirements:
    - Mandatory renewal every 6 months.
    - Password complexity (minimal length, special characters, …).
    - Inability to reuse previous password.
- Vulnerability management: regular software updates and if needed installation of hotfix patches.
- Final user can delete their own data at any time and deletion at the end of the contract is mandatory.
- Real-time anti-virus, anti-malware and anti-spyware protection.
- Administration tasks can only be performed from local network or via an Articque VPN access.
- Prevention systems.
- Data backup is scheduled and checked every working day.

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.

When a CUSTOMER needs to process personal or sensitive data, C&D Desktop and Articque Platform are the only suitable solutions applicable to this context. The C&D Online product is not suitable for this task. (cf. Art 12.7 of C&D Online 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.
- Wi-Fi access codes are regularly modified.
- Wi-Fi access uses the WPA2-TKIP protocol.
- Secure configuration is applied to all Articque devices (including smartphones).
- Internal password accounts are subject to the following requirements:
    - Mandatory renewal every 6 months.
    - Password complexity (minimal length, special characters, …).
    - Inability to reuse previous password.

Good practices to be applied to geocoding by THE CUSTOMER:

Users must never use 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