



Technical and Organisational Measures

TABLE OF CONTENTS

Confidentiality (Art 32 (1)(b) GDPR)	3
Access control	3
Measures to prevent data processing systems from being used by unauthorized persons	3
Measures to ensure that persons authorized to use a data processing system have access only to data subject to their right of access and that personal data cannot be read, copied altered or removed without authorization during processing, use and after storage	3
Measures to ensure that data collected for different purposes are processed separately	3
Integrity (Art 32 (1)(b) GDPR)	3
Handover control	3
Input control	4
Availability and resilience (Art 32 (1)(b) GDPR)	4
Availability control	4
Process for regularly testing, assessing and evaluating (Art 32 (1)(d) GDPR ; Art 25 (1) GDPR)	4
Privacy management	4
Data protection by design & default	5
Order control	5

Confidentiality (Art 32 (1)(b) GDPR)

Access control

The following measures shall ensure that unauthorized persons are denied access to the building or to the rooms of the data processing systems with which personal data are processed or used:

- Access control system through keys and badges for our offices in France and Romania
- Burglar alarm system for our offices in France and Romania
- Video surveillance for our offices in France and Romania

Measures to prevent data processing systems from being used by unauthorized persons

- Access only upon identification and authentication
- Unique assignment of user accounts and users
- Guideline for the secure, correct handling of passwords : we have a password policy describing these guidelines
- Regulation for mobile data processing systems or data carriers for employees having administrative privileges on the XWiki Cloud platform
- Access to internal services is protected through the use of an employee-only virtual private network

Measures to ensure that persons authorized to use a data processing system have access only to data subject to their right of access and that personal data cannot be read, copied altered or removed without authorization during processing, use and after storage

- Access logging and occasion-related analysis of log files
- Adaptation of security-relevant standard settings of new IT systems and applications and deactivation of unneeded security-relevant programs and functions
- Clear Desk/Clear Screen Policy
- Access-secure archiving of data

Measures to ensure that data collected for different purposes are processed separately

- Logical separation via access rules
- Separation of productive and test systems : production and non-production systems run on different machines, sometimes on different infrastructures (case of XWiki Cloud with the production pool and the demo pool)
- Linking records to a specific purpose

Integrity (Art 32 (1)(b) GDPR)

Handover control

Measures to ensure that data cannot be read, copied, altered or removed without authorization during electronic transmission or during their transport or storage on data carriers and to ensure that it is possible to verify and establish the places to which personal data shall be transmitted by data transmission equipment:

- Encrypted communication over secure networks in accordance with current security standards
- Safe disposal of data media that are no longer needed : for production data, this measure is handled by our sub-contractor OVH

- Prohibition of the use of hardware and software that has not been released : The XWiki build systems prevent the release of new product versions if it depends on any software library which have not been released in a final version. Our sub-contractor OVH is handling the validation of the hardware used to run our infrastructure.
- No forwarding of information to external IT services (private email addresses, unauthorized cloud storage)
- Specifications for employees for the use of data carriers : we train all XWiki employees on their digital hygiene yearly during the company annual seminar.

Input control

Measures to ensure that it can be subsequently verified and established whether and by whom personal data have been entered, modified or removed in data processing systems:

- Access to data processing systems only possible after login
- No passing on of passwords (password policy)
- Policy on how to proceed if a password becomes known (password policy)
- Analysis of log files for specific events

Availability and resilience (Art 32 (1)(b) GDPR)

Availability control

Measures to ensure that personal data are protected and available against accidental destruction or loss:

- Documented backup and recovery concept with regular backup and disaster-proof storage of data media : we have a procedure for backing up and restoring data both for our internal infrastructure and for our cloud platform. Backups are replicated in 3 different locations within the EU and are encrypted at rest and in transit.
- Use of security controls such as virus protection and firewalls : our infrastructure is secured with firewalls at its entry points. We are also running weekly virus and malware detection on instances hosted on our cloud platform.
- Storage systems with redundancy : our private cloud environment (used for hosting our infrastructure) uses RAID for ensuring redundancy on storage systems.
- Protection against fire, overheating, water damage, over-voltage and power failure in the server room : hardware protection is handled by our sub-processor OVH which have these measures in place.
- Use of uninterruptible power supply and emergency power generators : this is handled by our sub-processor OVH which have these measures in place.

Process for regularly testing, assessing and evaluating (Art 32 (1)(d) GDPR ; Art 25 (1) GDPR)

Privacy management

Measures to ensure that the technical and organizational measures taken remain effective in the long term:

- Regular monitoring of the technical and organizational measures taken : we are doing quarterly reports to CODIR
- Evaluation of messages and reports on unusual occurrences : we have put a process in place for handling security and privacy requests

- Training of employees in the handling of IT and IT security awareness : we have an annual conference at our seminar about security awareness

Data protection by design & default

Measures which are designed to implement data-protection principles, such as data minimization, in an effective manner:

- Data protection by default with regard to the scope of data processing
- Data protection by default with regard to the amount of personal data collected
- Data protection by default with regard to storage and deletion periods

Order control

Measures to ensure that personal data processed on behalf of the Customer are only processed in accordance with the Customer's instructions:

- Ensuring that orders are processed in accordance with instructions by dividing the responsibilities between Supplier and Customer : this is defined in our general conditions
- The Supplier's employees only have access to the information they need to carry out the order.
- Contract for processing in accordance with Art 28 GDPR must exist
- Obligation of the Supplier's personnel to comply with the data protection principles of Art 5 GDPR, in particular the confidentiality of data