Data Security and Privacy Statement

Document reference: GRC-DSPS
Document owner: Data Protection Officer — dpo@exalate.com
Classification: Public
Version: 2.1
Last updated: 14 October 2026
Review cycle: Annually, or on material change to processing activities

---

1. Introduction

This Data Security and Privacy Statement describes how Exalate NV ("we", "us", "our" or "Exalate") collects and processes your personal data in relation to your use of our website https://www.exalate.com/ and our cloud add-on services for various work management platforms.

Exalate respects your privacy and is committed to protecting your personal data in accordance with applicable data protection legislation, including the General Data Protection Regulation (GDPR), UK Data Protection Act 2018, Swiss Federal Act on Data Protection (FADP), California Consumer Privacy Act (CCPA), and other applicable laws.

By using our website or services, or by sharing your personal data with us, you acknowledge the manner in which we collect and process your personal data as described in this statement.

This statement should be read in conjunction with our Data Processing Agreement (DPA), which governs Exalate's role as a processor when processing personal data on behalf of our customers (licensees).

2. Controller Information

Exalate acts as data controller in respect of the personal data collected via our website and direct interactions. When providing synchronization services to licensees, Exalate acts as a processor under the terms of the DPA.

Company	Exalate NV
Registered Office	Ijzerenpoortkaai 3 bus 37, 2000 Antwerpen, Belgium
VAT	BE0834.937.594
Phone	+32(0)3.318.00.81
Email	info@exalate.com
Website	https://www.exalate.com
DPO Contact	dpo@exalate.com

3. Scope

This statement applies to:

Cloud Add-ons: Hosted services provided for various work management platforms including Atlassian (Jira, Confluence), ServiceNow, Salesforce, Azure DevOps, Zendesk, GitHub, and other supported platforms. Cloud Add-ons are delivered through respective marketplace frameworks and identified by the "Cloud" category in the corresponding marketplace listings.

Website: Our website at https://www.exalate.com/ and related web properties.

This statement does not apply to Server/Data Center Add-ons or on-premise deployments installed on client IT systems.

Single-Tenant Architecture: Exalate is a single-tenant application where a dedicated processing and storage environment is reserved for every tracker under sync. Each connected platform receives a dedicated Exalate node with its own isolated environment.

4. Definitions

Term	Definition
Personal Data	Any information relating to an identified or identifiable natural person, including name, email address, IP address, and other identifiers. Also includes "personal information" and "personally identifiable information" as defined by Applicable Data Protection Law.
Customer Data	All data created by end users and stored within connected work management platforms that is processed through Exalate
Data Subject	A natural person who is identified or identifiable by the Personal Data
Processing	Any operation performed on Personal Data, including collection, storage, use, disclosure, and erasure
Controller	Entity determining purposes and means of processing (Exalate for website data; Licensee for synchronized data)
Processor	Entity processing data on behalf of a Controller (Exalate when providing synchronization services)
Applicable Data Protection Law	Privacy, security, and data protection laws including GDPR, UK Data Protection Act 2018, UK GDPR, Swiss FADP, CCPA, and other applicable laws

5. Categories of Personal Data

5.1 Website Visitors and Software Users

Category	Examples
Personal Identifiers	Name, email, telephone
Professional Data	Company name, company domain
Electronic Identifiers	Device ID, IP address, Tracking ID
Usage Data	Usage statistics for Exalate nodes deployed on Exalate cloud

5.2 Synchronized Data

Categories of Personal Data included in data synchronized between work management tools are determined by the Licensee's configuration of the Software. Depending on how the Licensee has configured the Software, data processed may include sensitive data (such as medical data).

6. Data Processing Activities

6.1 Website and Communication

Purpose	Responding to inquiries, communicating with users via website or email (including helpdesk)
Data Types	Name, email, company, inquiry content
Legal Basis	Consent, legitimate interest
Retention	As long as necessary to fulfill the purpose; deleted upon request

6.2 Account Data

Purpose	License validation, contract administration, communication with customer instances
Data Types	AddOnKey, ProductType, ClientKey, BaseUrl, ServiceEntitlementNumber, SharedSecret, OauthClientId
Legal Basis	Contract performance
Retention	180 days after archiving of Exalate node

6.3 Operation Data

Purpose	Operation of the synchronization service
Data Types	License information, synchronization relations, twin and field traces, copies of latest and previous issue versions
Legal Basis	Contract performance
Retention	Deleted when no longer required for service provision

6.4 Customer Uploaded Data

Purpose	Storage of customer-created configurations and metadata
Data Types	Cloud Add-on configuration, metadata managed by Cloud Add-ons
Legal Basis	Contract performance
Retention	180 days after archiving of Exalate node

6.5 Session Data

Purpose	Product usage reporting, churn analysis and service improvement
Data Types	Usage statistics of service functionality
Legal Basis	Legitimate interest
Retention	2 years from the end of the customer relationship; thereafter retained only as de-identified aggregate data

6.6 Support Data

Purpose	Problem resolution via problem report functionality
Data Types	Account Data, Operation Data, Customer Uploaded Data collected via problem report
Legal Basis	Contract performance, legitimate interest
Retention	180 days after archiving of Exalate node or when no longer required

7. Data Storage and Location

Exalate Cloud is an infrastructure optimized for hosting Exalate nodes, implemented on top of multiple Kubernetes clusters running in multiple locations. Data residency can be chosen on a node-per-node basis. Contact sales@exalate.com for data residency requirements.

The locations are documented on our trust center at 'Exalate - Locations'

8. Data Security

We maintain state-of-the-art technical and organizational measures per GDPR Article 32 and other Applicable Data Protection Laws to ensure a level of security appropriate to the risk.

8.1 Applicable Data Protection Framework

Exalate complies with applicable privacy, security, and data protection laws including:

Jurisdiction	**Legislation**
European Union	General Data Protection Regulation (GDPR)
Belgium	Belgian implementing laws
United Kingdom	UK Data Protection Act 2018, UK GDPR
Switzerland	Swiss Federal Act on Data Protection (FADP)
California, USA	California Consumer Privacy Act (CCPA)

Additional jurisdictional requirements apply to the extent applicable to Exalate's processing activities.

8.2 Encryption

- All communication between Exalate nodes, connected platforms and Exalate Cloud infrastructure is encrypted in transit using current industry-standard transport encryption
- Databases and backups encrypted at rest using industry-standard algorithms

8.3 Access Controls

- Employee access limited to engineers requiring access for system maintenance
- Access based on principles of least privilege, need to know, and need to use
- Two-factor authentication required for infrastructure access
- Passwords protected irreversibly; employees cannot reconstruct passwords

8.4 Confidentiality

- All employees, contractors, and subcontractors execute confidentiality agreements
- Background screening for relevant employees
- Security awareness training on Security Policy
- Data separated per tenant; development and production environments fully separated

8.5 Endpoint Security

- Centrally managed endpoints with automatic device locking
- Automatic password policy enforcement
- Remote wiping capability for stolen/damaged equipment
- Anti-malware software and data loss protection

8.6 Network Security

- Multiple layers of controls (firewall, virus scanner, monitoring)
- Advanced user-, file-, and network-activity anomaly detection

8.7 Event Logging

- All access to servers and hosting providers monitored
- Audit logging activated on all relevant endpoints, servers, and equipment
- Log files retained for 90 days with regular internal audits. Shorter platform-enforced retention periods may apply to certain cloud-hosted services

8.8 Security Testing

- Annual penetration testing by independent external party
- Bug bounty program via BugCrowd platform for continuous security feedback

8.9 Business Continuity

- Business Continuity Plan established to recover IT systems in case of disruptive incident
- Daily backups with 3-day retention
- When a user account is deleted, personal data is erased in accordance with the disposal methods defined in Exalate's Data Management Policy. Residual copies held in backups are removed within the 3-day backup retention period

9. Access to Customer Data

Access to Customer Data is restricted to:

- Authorized Exalate employees
- Subcontractors from support and development teams

All subcontractors are contractually bound to the same data security and privacy standards that apply to Exalate under data processing agreements meeting GDPR requirements.

10. Sub-Processors

Exalate engages sub-processors for processing Personal Data. The current list of sub-processors is available at **trust.exalate.com**.

Changes to sub-processors are communicated in writing. Licensees have 30 calendar days to raise written objections to such changes per the DPA.

All sub-processors are subject to substantially the same data protection obligations as set out in the DPA. For sub-processors in third countries, appropriate safeguards (e.g., EU Standard Contractual Clauses) are implemented.

11. International Transfers

11.1 Processing Locations

Data can be stored in different locations as documented in 'Exalate Locations'. The default is Europe. Any other locations is only possible after agreement and/or configuration implemented by the customer.

For instance if a node resides in the US and a synchronisation is being configured between EU and the US, there will be an international transfer.

11.2 Transfer Safeguards

For transfers of Personal Data to countries outside the EEA without an adequacy decision, Exalate ensures appropriate safeguards in accordance with the GDPR:

- Standard Contractual Clauses (SCCs) adopted by the European Commission
- Adherence to approved codes of conduct (Article 40 GDPR)
- Approved certification mechanisms (Article 42 GDPR)
- Reliance on adequacy decisions (e.g., Switzerland)
- Other appropriate mechanisms ensuring adequate protection

11.3 Data Residency Options

Data residency can be selected on a node-per-node basis. Organizations requiring EEA-only data processing should contact sales@exalate.com to configure appropriate data residency.

11.4 UK and Swiss Transfers

For transfers from the United Kingdom, the UK International Data Transfer Agreement (IDTA) or UK Addendum to EU SCCs applies. For transfers from Switzerland, the Swiss Federal Act on Data Protection (FADP) requirements are observed.

Contact us for information on specific transfer mechanisms.

12. Data Breach Notification

Upon becoming aware of a Personal Data Breach, Exalate notifies affected Controllers without undue delay, but no longer than seventy-two (72) hours after becoming aware.

Exalate cooperates with Controllers in investigating breaches and provides information reasonably necessary for reporting to supervisory authorities.

13. End of Subscription

Upon unsubscription from Cloud Add-ons:

1. Stored Customer Data is marked for deletion
2. Data is deleted within 180 days after archiving of Exalate node
3. Earlier deletion available upon customer request
4. Unless storage is mandatory under applicable laws, data is erased or returned to Controller at Controller's option
5. Usage and session data processed for product usage reporting, churn analysis and service improvement is retained for 2 years from the end of the customer relationship, after which identifiers are removed and only de-identified aggregate data is retained. This period applies in place of the 180-day deletion window described above.

14. LLM (AI) Integration

Exalate functionality includes processing of connection configurations through an LLM-based agent. The agent processes connection configuration and synchronisation script content in order to extract human-readable explanations and propose integration improvement suggestions.

Issue payloads, field values, attachments, comments and any other synchronised Customer Data are not sent to the LLM-based agent.

15. Your Legal Rights

15.1 Rights Under GDPR (EU/UK)

Under GDPR Articles 15-22 and UK GDPR, you have the following rights:

Right	Description
Access	Obtain confirmation of processing and access to your personal data, including a copy
Rectification	Correct inaccurate or incomplete personal data
Erasure	Request deletion of personal data in specific circumstances ("right to be forgotten")
Restriction	Limit processing in specific circumstances
Portability	Receive your data in structured, commonly used, machine-readable format
Object	Object to processing based on legitimate interest for reasons relating to your specific situation

15.2 Rights Under CCPA (California Residents)

California residents have additional rights under the CCPA:

Right	Description
Know	Right to know what personal information is collected, used, shared, or sold
Delete	Right to request deletion of personal information
Opt-Out	Right to opt-out of the sale of personal information (Exalate does not sell personal information)
Non-Discrimination	Right not to be discriminated against for exercising privacy rights

15.3 Exercising Your Rights

Exercise of these rights is free of charge. Unreasonable or repeated requests may incur reasonable administrative fees (notified in advance).

Exercise your rights by emailing: **dpo@exalate.com**

Clearly specify which right you wish to exercise. Additional information may be required to verify identity.

Response time: 1 month (extendable to 3 months with notification of reasons). For CCPA requests: 45 days (extendable by an additional 45 days with notice).

16. Supervisory Authorities

If you consider that processing of personal data infringes applicable data protection law, you have the right to file a complaint with a supervisory authority.

16.1 Belgium (Lead Supervisory Authority)

Authority	Gegevensbeschermingsautoriteit / Autorité de protection des données
Website	www.gegevensbeschermingsautoriteit.be
Address	Drukpersstraat 35, 1000 Brussels, Belgium
Phone	+32 (0)2 274 48 00
Email	contact@apd-gba.be

16.2 Other Jurisdictions

Jurisdiction	**Authority**
United Kingdom	Information Commissioner's Office (ICO) - ico.org.uk
Switzerland	Federal Data Protection and Information Commissioner (FDPIC) - edoeb.admin.ch
California, USA	California Attorney General - oag.ca.gov

Contact Exalate first to address concerns before approaching the authority.

17. Cookies

Our website uses cookies and similar technologies, including cookies set by third-party analytics and advertising providers. The cookies used, their purposes and their retention periods, together with the options for managing your preferences, are available through the cookie settings on our website. For questions about our use of cookies, contact dpo@exalate.com.

18. Third-Party Links

Our website and services may contain links to third-party websites and applications. Exalate is not responsible for their content or privacy practices. Review third-party privacy policies before accepting their cookies or visiting their websites.

19. Personal Data of Third Parties

If you share third-party personal data with us, you guarantee that you have informed those parties and obtained all necessary consents to communicate their personal data to Exalate.

20. Liability

Exalate is not liable for unlawful processing by third parties to whom data has been legitimately transmitted (excluding processors/sub-processors).

Exalate is liable only for damage caused by processing if it did not comply with its specific GDPR obligations. Exalate is not liable for special, incidental, indirect, or consequential losses or damages to the maximum extent permitted by applicable law.

21. Changes to This Statement

This statement may be amended periodically. Changes will be notified on our website.

Amended versions take effect ten (10) days after publication, unless such modifications are necessary to comply with legal requirements, in which case changes take effect immediately.

22. Related Documents

Document	Location
Data Processing Agreement (DPA)	Available at trust.exalate.com or upon request
Sub-Processor List	trust.exalate.com
Processing Locations	trust.exalate.com
Cookie Policy	Section 17 of this statement

23. Contact

For questions about this statement, privacy matters, or data processing:

DPO Email	dpo@exalate.com
General Email	info@exalate.com
Sales (Data Residency)	sales@exalate.com
Phone	+32(0)3.318.00.81
Website	https://www.exalate.com
Trust Center	trust.exalate.com