GDPR REPORT PASSBOLT

July 2026

Name	Status	Modifications	Date
Clémence Philippe	Drafter		June 2026
Clémence Philippe	Drafter		July 2026

Versions control

1. Overview of Passbolt Activities

Passbolt S.A. is a cybersecurity company incorporated under the laws of Luxembourg, specializing in the management of credentials, secrets, and access for professional organizations, critical infrastructures, and development teams.

The entity benefits from the official "Made in Luxembourg" label and operates fully within the strict regulatory framework of the European Union.

Released under the AGPLv3 open-source license, the Passbolt solution features fully transparent, auditable, and publicly verified source code by the international security research community. This attribute eliminates the risk of inserting undocumented features or backdoors, meeting the most stringent requirements of public procurement and defense policies.

The security of the solution is based on the native end-to-end implementation of the OpenPGP (GPG) standard. The protocol implies that the server has, at no time, the knowledge or capacity to decrypt stored secrets since it never holds the keys required to access them locally. Authentication and decryption take place locally on the client workstation using the user's private key. An anti-phishing mechanism, materialized by an individualized cryptographic visual token, completes the access control system.

2. Certifications

Passbolt holds several American and international security certifications:

- **SOC 2 Type II**: Passbolt has successfully passed the SOC 2 Type II compliance audit (developed by the AICPA). This certification attests to the maturity and effectiveness of their internal controls regarding the security, availability, and confidentiality of data over time.
- **European Sovereignty and Quality Labels:**
    - **"Made in Luxembourg":** Passbolt was awarded this official label by the Luxembourg Chamber of Commerce. It certifies the company's local roots and the sovereign design of the product within the Grand Duchy.
    - **"Cybersecurity Made in Europe":** Passbolt holds this label issued by the ECSO (European Cyber Security Organisation), guaranteeing that the company is legally based in Europe, that it complies with European data protection standards (GDPR), and that it is not subject to extraterritorial legislation (such as the American *Cloud Act*).
    - **the infrastructures hosting the Passbolt Cloud** (whether for the *Business Cloud* or the *Sovereign Cloud* in Luxembourg) all benefit from the strictest certifications:
        - **ISO 27001** (Information Security Management)

- **ISO 27017 & ISO 27018** (Cloud security and privacy)
- **GDPR Compliance** with strict hosting on European soil.

3. Audit results

3.1. Scope

Examin conducted GDPR audit of the technical and regulatory compliance documentation prepared by Passbolt, available on the Secureframe platform under the "Governance" tab.

The goal was to provide an assessment of the steps taken to ensure Passbolt's compliance with the GDPR.

3.2. General evaluation of the documentation

Analysis of the documentation shows that Passbolt has drafted many documents allowing it to prove its compliance with the GDPR.

The fundamentals are established, and the technical and organizational measures relating to the security of the information system are very robust, strict, and ensure a high level of security for both Passbolt's personal and commercial data.

Passbolt has numerous documents governing its technical and organizational governance: Information Systems Security Policy, incident management, risk management, code of conduct, management of IT tools and networks, ISMS, data retention, physical security, supply chain control, compliance with DORA regulations, crisis management, BCP...

3.3. Evaluation of the documentation regarding GDPR

We have analyzed several documents relating to GDPR compliance and have several remarks:

- **HR Policy:**

Some information (e.g. contact details of the DPO and the CNPD) is missing and a new version will be drafted.

Employees will also be informed of their rights (access, restriction, rectification, portability, objection, etc.).

Certain clauses need to be clarified, particularly those regarding "service providers" and data access by local authorities, especially US authorities.

- **Data Retention policy**

The rules established in the policy only concern customer data, and information is missing on the retention periods for other types of data: data collected via the website, HR data, accounting data, providers and suppliers data...

This Policy deserves to be completed to be more exhaustive.

- **DPO Nomination**

Due to the nomination of Examin as DPO, the Privacy and Data Protection Policy must be modified to include the DPO's contact details.

- **DPA (Data Processing Agreements)**

We reviewed the DPA available for Passbolt clients on the website. We also reviewed the DPAs signed with sub-processors located in the EU and outside the EU. The templates comply with the GDPR.

- **Website:**

Regarding the website, we have reviewed the "Website Privacy Policy": it is recommended to add a paragraph on the possibility of contacting the CNPD (compliance with Article 13 of the GDPR).

Regarding the "legal terms," it would be good to add the contact details of the website host: registered office address and telephone number, as well as the name of the publication director of the website within Passbolt.

SYNTHETIC SECTION

1. Overview of the Passbolt solution

The Passbolt solution is released under the AGPLv3 open-source license. Its source code is described as transparent, auditable, and publicly verifiable by the international security research community. This transparency is presented as reducing the risk of undocumented features or backdoors.

The security architecture of the solution is based on the native end-to-end implementation of the OpenPGP / GPG standard. The server does not have knowledge of, or the capacity to decrypt, stored secrets.

Authentication and decryption take place locally on the client workstation using the user's private key. The access control system is completed by an anti-phishing mechanism based on an individualized cryptographic visual token.

For the purposes of a privacy impact analysis, data controllers should therefore take into account that the solution is intended to manage credentials, secrets, and access information, and that the documented security model relies on open-source transparency, end-to-end cryptography, local decryption, and a server architecture in which the provider has no technical means of accessing or decrypting users' data.

2. Overview of the treatment

In the context of credentials, secrets and access management, the role of Passbolt is to provide a cybersecurity solution for professional organizations, critical infrastructures and development teams.

The processing is based on the use of the Passbolt solution to manage credentials, secrets and access information. These elements are protected through an end-to-end cryptographic architecture based on the OpenPGP / GPG standard. The server does not have knowledge of the stored secrets. It does not have the capacity to decrypt them.

Authentication and decryption take place locally on the user's workstation. This is done using the user's private key. The access control mechanism is complemented by an anti-phishing mechanism. This mechanism is based on an individualized cryptographic visual token.

The solution is released under the AGPLv3 open-source license. Its source code is described as transparent, auditable and publicly verified by the international security research community. This transparency is intended to reduce the risk of undocumented features or backdoors.

For the purposes of a privacy impact analysis, the processing should therefore be understood as the secure management of credentials, secrets and access information through an open-source and end-to-end encrypted solution. The data controller should assess this processing in light of no technical capability to access users' data , the local decryption model and the cryptographic access control mechanisms described by Passbolt.

3. Assessment of measures ensuring the proportionality and necessity of processing

3.1 Explanation and justification of the purposes

Purposes	Legal basis
Provision of a collaborative password and credential management service enabling authorized users to generate, store, organize, access, share, and manage professional credentials and secrets.	Contract

3.2 Explanation and justification of data minimization

Details of data processed	Details of data processed	Details of data processed	Details of data processed
Passwords, private keys and other credentials.	Authentication data and professional secrets	The data is needed to allow authorized users to generate, store, organize, access, share and manage professional credentials and secrets.	The server has no knowledge of the stored secrets. It has no capacity to decrypt them. The solution uses end-to-end OpenPGP / GPG encryption. Decryption takes place locally on the user workstation.
User private key used for local authentication and decryption	Cryptographic data	The private key is needed to authenticate the user and decrypt secrets locally. It supports the Zero-Knowledge security model.	Decryption is performed locally on the client workstation. The server is not given the ability to decrypt stored secrets

IDs, keys or other unique credentials used to identify the account holder	Identification and access management data	The data is needed to identify authorized users.	Users are provided with unique accounts. Shared accounts are limited.
Access rights, permission levels and account privileges assigned to users	Authorization and access rights data	The data is needed to restrict access to the credentials and secrets.	Access is based on the principle of least privilege. Users receive minimum access according to their job function, business requirements or need-to-know
Information used to create, modify or revoke access during onboarding, role changes and offboarding	Account lifecycle management data	The data is needed to manage user access throughout the account lifecycle	Onboarding and offboarding steps are documented. Access must be revoked within 24 hours of the user's last day, or sooner if necessary. Access changes must be tracked through ticketing or document management tools.
Customer data needed to maintain an active account or perform the agreement with the customer	Customer relationship and account data	The data is needed to provide the service while the customer account is active	Customer data is retained only while the account is active or according to the agreement with the customer

3.3 Accurate and up-to-date information

Measures for data quality	Justification
Client-side maintenance of credentials and secrets entered into Passbolt	Passbolt is used to generate, store, organize, access, share and manage professional credentials and secrets. Since the solution is based on a Zero-Knowledge model, the server does not have knowledge of the stored secrets. It cannot decrypt them. As a result, the accuracy of the content of the credentials and secrets must be maintained by the Client and its authorized users.
Local authentication and decryption by the user[1]	This supports the integrity of the access process. It ensures that access to secrets depends on the user's cryptographic material. It also limits Passbolt's ability to view or correct the content of stored secrets.
Unique user accounts and traceability of account activity	Unique accounts support reliable identification of users. They reduce ambiguity over who created, accessed, modified or shared credentials and secrets.
Access rights defined according to role, business need and need-to-know	Ensure that access information remains relevant and proportionate. It reduces the risk that users keep access rights that are no longer accurate or justified.
Documented onboarding process	Ensures that access rights are based on documented business needs before the user receives access to the service.
Documented offboarding process and access revocation	Ensures that user access remains up to date. Prevents former users from retaining access to credentials, secrets or related systems after their role has ended.
Customer data retained according to account status and agreements	Links retention to the active customer relationship and to the applicable contractual framework.
Disposal of customer data following a customer request	Supports the correction of the data environment when the customer relationship or customer request no longer justifies retention.

[1] Authentication and decryption take place on the client workstation using the user's private key.

3.4 Explanation and justification of retention periods

Data types	Retention period	Justification for the retention period	Mechanism for deletion at the end of the retention period
Professional credentials and secrets stored in the Passbolt workspace	For as long as the customer chooses to use the service, or for as long as the customer account is active[2]	data is needed to allow authorized users to store, access, share and manage professional credentials and secrets during the customer's use of the service	For Passbolt Cloud, once the customer terminates the cloud account, data is automatically deleted from backups within 6 weeks.
Customer account data and customer relationship data needed to provide the service	For as long as the account is active or in accordance with the agreement between Passbolt and the customer	The data is needed to maintain the customer account and provide the service	Customer data is disposed of within 60 days of a request by a current or former customer
Access rights, permissions and account privileges	The data is retained while the user needs access to the service, and reviewed when the role changes or the account is no longer required.	The data is needed to apply the principle of least privilege. They ensure that user only receive access based on job function, business requirements or need-to-know.	Access changes must be documented and approved. When an employee or contractor leaves, access must be revoked within 24 hours of the last day, or sooner if necessary. Access rights are also reviewed and reallocated when roles change or accounts are no longer required.
Audit logs and alerts from production systems, applications, databases, servers, message queues, load balancers, critical services, IAM user	Minimum retention of 1 year. If logs contain PII and cannot be anonymized, the retention period is set to 60 days.	Logs are retained to support troubleshooting, auditing, capacity planning and potential forensic investigations	Logs are securely stored and archived. Access controls are used to prevent unauthorized access, deletion or tampering. Where logs contain PII and cannot be anonymized, the shorter

[2] The retention may also depend on the agreement between Passbolt and the customer

activity and administrator activity.			60-day retention period applies.
Database backups containing customer data or service data.	The maximum allowable retention period for a database backup is 3 years. For Passbolt Cloud, customer workspace data is automatically deleted from backups within 6 weeks after termination of the cloud account.	Backups are retained to ensure business continuity and disaster recovery. They are used to protect the availability, integrity and confidentiality of stored data in case of disruption or data loss.	Backups are periodically tested. Backup systems and media protect the confidentiality, integrity and availability of stored data. For Passbolt Cloud, deletion from backups occurs automatically within 6 weeks after account termination.

3.5 Assessment of measures

Measures ensuring the proportionality and necessity of processing	Acceptable / Needs improvement	Corrective measures or explanations
Purposes: specific, explicit, and legitimate	Acceptable	/
Legal basis: lawfulness of processing, prohibition on use for other purposes	Acceptable	/
Data minimization: adequate, relevant, and limited	Acceptable	/
Data quality: accurate and up to date	Acceptable	/
Shelf life: limited	Acceptable	/

4. Assessment of measures to protect the rights of data subjects

4.1 Information for data subjects

In the context of the Passbolt service, the information of data subjects must be assessed according to the role of the solution. Passbolt provides a collaborative service for the management of credentials, secrets and access. The service is based on an architecture in which the provider has no technical means, at any stage, of accessing or decrypting users' data. The server does not have knowledge of the stored secrets and cannot decrypt them.

The information provided to data subjects should therefore cover the processing that is relevant to the use of the service. This includes the purpose of the processing, the categories of data processed, the retention periods, the recipients or categories of recipients, the applicable security measures, and the rights available to individuals.

Where the data is collected directly from the individual, the information is provided at the time of collection. Where the data is not obtained directly from the individual, the information is provided within a reasonable period and, in any event, within one month. The routes are available for individuals wishing to exercise their rights regarding personal data.

As the service provider, Passbolt makes available technical and organizational information that can support the controller's transparency obligations. This includes information on the , encryption, access control, retention, logging, and data protection governance.

Mesures pour le droit à l'information	Implementation methods	Justification / assessment
Express consent at registration	*Privacy and data protection policy*	/
A detailed description of the purposes of data processing (specific objectives, data matching where applicable, etc.)	*Privacy and data protection policy*	/
Detailed overview of the personal data collected	*Privacy and data protection policy*	/
Overview of the data subject's rights (right to erasure, etc.)	*Privacy and data protection policy*	/

Information on secure data storage, particularly in the case of outsourcing	*Privacy and data protection policy*	/
Company contacts details (name and contact information) for privacy enquiries	*Privacy and data protection policy, legal notice*	/
Where applicable, the data subject shall be informed of any changes relating to the data collected, the purposes for which it is used, and the confidentiality provisions	*Privacy and data protection policy*	/

4.2 Consent

Measures for consent collection	Implementation methods	Justification / assessment
Express consent at registration	Where appropriate, consent is obtained from the data subject before collecting and processing their data	General consent mechanism
Segmented consent by category of data or type of processing	N/A	/
Express consent before sharing data with third parties	N/A	/
Consent presented in a way that is easy to understand and tailored to the person concerned (particularly in the case of children)	N/A	/
Obtaining parental consent for children under the age of 13	N/A	/

If the account has not been used for a long time, ask the person concerned to reaffirm their consent	N/A	/
If the user has consented to the processing of specific data (e.g. their location), the interface clearly indicates that such processing is taking place (icon, indicator light)	N/A	/
If the user changes their contract, the settings relating to their consent are retained	N/A	/

4.3 Exercising the right of access

The exercise of data subjects' rights of access and portability remains purely theoretical in this context.

Measures for the exercise of access rights	Justification
Possibility to access all personal data relating to the data subject	**For internal users:** The users can log in to their Passbolt account to view all data concerning them, including transcriptions, recordings, profile information, and any other data associated with their account. **For external individuals:** Where necessary, data subjects may submit an access request to the data controller through customer support or the DPO. The data controller will provide either the requested data or, where applicable, access to the conversation via a shared link. A dedicated procedure is in place to respond to such requests in accordance with the right of access provided under the GDPR, in particular Article 15.
Possibility to securely consult usage traces linked to the data subject	Audit logs and alerts are collected and monitored for production systems, applications, databases, servers, critical services, IAM user activity and administrator activity. Logs are securely stored and archived. Access control is used to prevent unauthorized access, deletion or tampering. Logs may be made available to relevant team members for troubleshooting, auditing and capacity planning.
Possibility to download an archive of all personal	N/A

data relating to the data subject	

4.4 Exercising the right of access and the right to data portability

Measures relating to the right to data portability	Justification
The ability to retrieve, in a format that is easily reusable, the personal data identified by the data subject, so that it can be transferred to a third-party service	N/A

4.5 Exercising the rights to rectification and erasure

Measures concerning the rights to rectification and erasure	Justification
Possibility to rectify personal data	Authenticated users can correct information stored in Passbolt resources. The users can edit a password directly from the password workspace. If the personal data concerned relates to the user account or to information held by Passbolt outside the customer workspace, the data subject may contact Passbolt directly to rectify the information, where applicable.
Possibility to delete personal data	Users or administrators may delete password resources stored in Passbolt, subject to their access rights. When a user is deleted, the resources solely owned by that user and not shared are also deleted. If the user owns shared resources or is the sole manager of a group, ownership or management must be transferred before deletion in order to preserve access and data integrity. For Passbolt Cloud, upon the customer's instruction or termination of the agreement, Passbolt must return or delete personal data within 30 business days, unless otherwise agreed or unless retention is required by law.

List of personal data that will be retained regardless (due to technical constraints, legal obligations, etc.)	Certain data must be retained for legal or technical reasons, including to comply with contractual, tax, or claims management obligations
Implementation of the right to be forgotten for minors	N/A

4.6 Exercising the rights to restrict processing and to object

Measures concerning the rights of restriction and objection	Justification
Existence of “Privacy” settings	Non applicable
Invitation to change the default settings	Non applicable
“Privacy” settings available during registration	Non applicable
“Privacy” settings available after registration	Non applicable
Measures for the rights to restriction and objection	Passbolt provides features enabling the customer to restrict the processing of personal data where necessary. The customer can limit access to credentials and related personal data by managing user roles, groups and resource permissions, by revoking or modifying sharing rights, or by deleting resources or user accounts where appropriate.
Compliance regarding tracking technologies, such as cookies or advertising	Non applicable
Exclusion of children under 13 from automated profiling	Non applicable

Effective cessation of user data processing upon withdrawal of consent	Where consent is used, individuals are informed of their right to withdraw consent

4.7 Subcontracting identified

Contracted processor	Processor activities	Type of personal data	Headquarters location	Implemented safeguards & data transfer mechanism	Data Hosting Location
Aikido	Web Application Firewall	IP	Belgium	ISO 27001:2013, ISO 27017:2015, and ISO 27018:2019 certifications.	EU/USA
Amazon Web Services	Email delivery, AWS SES	Name, email address, location, IP address of customer and authorized users	USA	ISO 27001:2013, ISO 27018, ISO 27701, SOC 2 certifications. Standard Contractual Clauses. Using services located in Ireland and Germany.	EU
Chargebee	Subscription and invoice management	Name, email address, location, IP address of customer	USA	ISO 27001:2013, SOC 1, SOC 2, PCI DSS certifications. Standard Contractual Clauses. Using a data center located in Europe.	EU
ChartMogul	Subscription and invoice management	Name, email address, location, IP address of customer	Germany	SOC 2 Type II. Standard Contractual Clauses.	EU
Cloudflare	Web Application Firewall and Content Delivery Network	Name, email address, location, IP address of	USA	ISO 27001:2013, SOC 2 Type II, SOC 3, PCI DSS 3.2.1 certifications. Standard Contractual Clauses.	EU/USA

		customer and user of service			
Google Cloud Platform, GCP	Hosting of Passbolt websites and cloud data	Name, email address, credentials, location including IP address of cloud service users	USA	ISO 27001, ISO 27017, ISO 27018, ISO 27701, SOC 1, SOC 2, SOC 3, PCI DSS certifications. Cloud site data is hosted in Belgium and Germany. Standard Contractual Clauses.	EU
HubSpot	Customer relationship management and support	Name, email address, address of customer	USA	Security best practices and infrastructure providers with SOC 2 Type II and ISO 27001 certifications. Standard Contractual Clauses.	USA
n8n	Integration platform	Name, email address, address of customer, IP, support request data	Germany	SOC 2 Type II.	EU
New Relic	Performance and security monitoring	Log information, which may contain email and name of customer and service user	USA	SOC 2 Type II certification. Standard Contractual Clauses.	USA
Odoo	Accounting	Name, email address, location of customer	Belgium	SOC 1, SOC 2 Type II audited reports, CAIQ v3.1. Relies on data centers with ISO 27001 certification. Data protection clauses in contract. EU hosting location.	EU
Slack	Support and alerts	Name, email, IP, support request data/logs	USA	ISO 27001, ISO 27017, ISO 27018, SOC 2, SOC 3 certifications. Standard Contractual Clauses.	USA

Stripe	Payment management	Name, email address, location, credit card of customer	USA	PCI Service Provider Level 1 certification. Standard Contractual Clauses.	USA
Thales Cyber Solutions Luxembourg	Security Operation Center / Computer Security Incident Response	Location including IP address of cloud service users; log information, which can contain email and name of customer and service user	Luxembourg	ISO 27001:2013 certification.	EU
Zoho	Accounting	Name, email address, location of customer	USA	ISO 27001:2013, ISO 27701, ISO 27017, ISO 27018, ISO 9001, SOC 2 Type II, PCI DSS certifications. Standard Contractual Clauses.	EU

4.8 Assessment of measures

Measures ensuring the proportionality and necessity of processing	Acceptable / Needs improvement	Corrective measures or explanations
Information for data subjects (fair and transparent processing)	Acceptable	/
Collecting consent	Acceptable	/
Exercising the right of access and the right to data portability	Acceptable	/
Exercising the right to rectification and erasure	Acceptable	/
Exercising the rights to restrict processing and to object	Acceptable	/
Subcontracting to third parties: identified and formalized in a contract	Acceptable	/
Data transfers: Compliance with obligations regarding data transfers outside the European Union	Acceptable	