

# Patronum+

## Service Definition

Your  
**Google**  
Workspace  
Manager



## TABLE OF CONTENTS

|                                                      |    |
|------------------------------------------------------|----|
| 1. PATRONUM+                                         | 3  |
| 2. KEY PRODUCT FEATURES                              | 4  |
| 2.1 Automated file-sharing governance and compliance | 4  |
| 2.2 End user file compliance and remediation         | 4  |
| 2.3 Automated data retention and file expiry         | 4  |
| 3. SERVICE OVERVIEW                                  | 6  |
| 3.1 Operations                                       | 6  |
| 3.2 Privacy and Data Protection                      | 6  |
| 3.3 Installation and 30-day Free Trial               | 7  |
| 3.4 Deinstallation                                   | 7  |
| 4. PATRONUM LICENSING                                | 8  |
| 5. ABOUT BESPIN LABS                                 | 9  |
| 6. PATRONUM+ FEATURE LIST                            | 10 |
| 6.1 Allow Domain List                                | 10 |
| 6.2 Workflow                                         | 10 |

## 1. PATRONUM+

Patronum+ includes all the core functionality of Patronum, together with file governance and compliance capabilities. It enables IT administrators and data security teams to protect file data, and automate the safeguarding of files shared both internally and externally.

Patronum+ simplifies security, reduces risks, promotes collaboration with end users and ensures continuous compliance - all in a single interface.

Patronum (see Patronum Google Workplace Manager Service Description) fills in the gaps that exist in Google's Workspace Admin Console. Patronum enables your organisation's IT and security teams for example to centrally automate tasks such as onboarding and offboarding staff, monitoring and enforcing file sharing and enabling organisation contact sharing to mobile devices.

Patronum and Patronum+ software are supplied to customers as software as a service, just like Google Workspace. This means your organisation along with all our other customers will experience exactly the same operational infrastructure and procedures, product features, performance, security and support from Bespin Labs.

Google Workspace administrators may use either Patronum or Google Admin Console at any time so an organisation is not wholly dependent on Patronum - it is not business critical.

We do not offer bespoke versions of Patronum or customised operating procedures or personalised support in order to keep Patronum subscription costs as low as possible.

You can learn more about Patronum and Patronum+ functionality in our Product Documentation at - <https://help.patronum.io/en>.

## 2. KEY PRODUCT FEATURES

Patronum+ includes all functionality provided in Patronum (as described in the Patronum Google Workspace Manager Service Description), together with additional file governance and compliance features. These capabilities are delivered through the creation of sophisticated file policies that define the scope, conditions, and actions to be applied to files. See Section 6 for a detailed list of Patronum+ features.

### 2.1 Automated file-sharing governance and compliance

Patronum+ enables automated file policies to prevent unauthorised access to sensitive data by revoking cloud file access and locking down files. Shared drives and folders are often aligned to specific groups, with Patronum+ policies used to govern how files can be shared - for example, preventing the sharing of certain file types or restricting access to read-only.

Sharing policies can also take organisational roles into account, determining whether an end user has sufficient privileges to share content externally. Patronum+ policies both enforce these controls and detect potential risks, automatically correcting issues where appropriate.

Sharing restrictions filters can identify files that match defined criteria, including: internal sharing, external sharing, sharing with gmail.com accounts, sharing with any domain outside an allowlist, sharing with anyone at the domain via a link, or sharing with anyone in a target audience via a link.

### 2.2 End user file compliance and remediation

Patronum+ helps keep your environment secure by notifying users when they breach your organisation's file-sharing policies. However, security is a shared responsibility, and a collaborative approach with file owners is preferred.

Patronum+ can be configured to periodically notify end users about files they have shared and prompt them to review access via a dedicated dashboard. End users can then confirm whether external access to files they own remains appropriate, defer action by snoozing files or update the sharing settings as needed.

### 2.3 Automated data retention and file expiry

Organisations are often required by national laws or sector regulations to retain data for a fixed period, or conversely to keep data only for as long as is strictly necessary for data protection purposes. These requirements can be implemented using file expiry policies in Patronum+.

File expiry policies enable external access to files to be revoked or files to be automatically deleted after a specified period or on a defined date. Patronum+ policies can be applied to specific groups, folders, or other file ownership criteria, ensuring data is managed and disposed of in line with regulatory and organisational requirements.

## 3. SERVICE OVERVIEW

### 3.1 Operations

#### Service Operator

Bespin Labs Ltd, Bates Mill, Colne Road, Huddersfield, HD1 3AG United Kingdom.

#### Service Access

Patronum+ is a subscription based software as a service product installed within a customer's Google Workspace domain by a Super Admin via the Google Workspace Marketplace. User access to Patronum+ is determined by customer's admin delegation and permissions.

#### Support Services

Support is available within Patronum+ or at - <https://www.patronum.io/support/>.

- Online chat available 24/7 all year round
- Video call
- Screen sharing

Help is available from within Patronum+ or at - <https://help.patronum.io/en/>.

#### Hosting & Location

Patronum runs in Google App Engine on Google Cloud Platform's data centres located in UK and EU countries.

#### Service Availability

Google App Engine's service level objective is a monthly uptime percentage of at least 99.95%.

#### Service Security

As specified in "Patronum - Google Workspace Manager by Bespin Labs" Government Digital Marketplace entry and Google Cloud Platform security details at - <https://cloud.google.com/docs/security>.

### 3.2 Privacy and Data Protection

Bespin Labs processes general contact data according to the Privacy Policy at <https://www.bespinlabs.com/privacy-policy>.

Patronum+ is supplied and operated according to the Master Subscription Agreement (MSA) at - <https://patronum.io/master-subscription-agreement> .

Patronum+ data protection is specified in the Data Processing Agreement (DPA) at - <https://patronum.io/data-processing-agreement> .

Patronum+ is operated in a secure multi-tenant cloud environment on Google Cloud Platform with all customers sharing a common robust operational infrastructure, software, security and support under the same MSA and DPA.

It is important to note that Patronum+ access is based on the permissions set and controlled by an organisation's IT and security teams and Bespin Labs personnel cannot and will not access the content of customer documents or emails.

### 3.3 Installation and 30-day Free Trial

Any Google Workspace domain may be registered at <https://www.patronum.io> for a 30-day free trial of Patronum+. After submitting a short form you will be emailed details about how to install Patronum+ on your domain. You will need Super Admin privileges to fully install Patronum+ on your organisation's domain.

Some Patronum and Patronum+ features will fully operate when Patronum+ is first installed. However in the context of a substantial organisation there are certain background tasks that may require up to 24 hours to complete such as the extraction of file metadata of every file in the organisation's Google Drives or acquisition of the organisation's contact directory, and during this time the Patronum and Patronum+ features that depend on this data will be locked until the processing is complete.

Patronum+ co-exists with Google Admin Console so you may use either at any time.

### 3.4 Deinstallation

Patronum+ must be removed by a Google Workspace domain Super Admin.

After Patronum+ has been fully deinstalled any Workspace Data previously added or updated in your Google Directory or Google Drives will remain unchanged in its current state. Your Google Workspace domain will continue to operate normally and we will permanently delete any Patronum+ Data accumulated in use within 30 days.

## 4. PATRONUM LICENSING

For pricing details please refer to the Patronum Pricing Plan. The minimum subscription period is one year.

Patronum licensing is based on a per user annual subscription paid in advance depending on the Google Workspace licence types and number of user licences in a domain as follows:

- (a) A Patronum or Patronum+ Business User subscription is required for every Google Workspace Business/Enterprise user licence, whether allocated to an active user account or not;
- (b) A Patronum or Patronum+ Frontline Worker subscription is required for every Google Workspace Frontline user licence, whether allocated to an active user account or not;
- (c) A Patronum Archive User subscription for every Google Workspace archive user licence or Patronum archive user in an organisation's Google Cloud storage bucket;
- (d) A Patronum or Patronum+ Education User Subscription for every Google Workspace Education active user licence;
- (e) A Patronum or Patronum+ Nonprofit User Subscription for every Google Workspace Nonprofit active user licence;
- (f) Education/Nonprofits Google Workspace non-live and archive users are given access to Patronum free of charge;
- (g) Education and Nonprofits eligibility is designated by Google;
- (h) There are no retrospective Patronum subscription adjustments for user changes for an organisation's domain during the previous Subscription Term.

## 5. ABOUT BESPIN LABS

Bespin Labs Limited is a UK Google Cloud solutions provider. It became an Official Google Cloud Partner in 2018 and launched its first product, Patronum in 2019.

Patronum is operated as software as a service exclusively on Google Cloud Platform in the UK and Europe.

Bespin Labs runs in a transparent, collaborative, and engaging community way for our team, partners and our customers. The customer first approach is at the heart of everything the company does, from features requests to pricing strategies.

## 6. PATRONUM+ FEATURE LIST

Compliance Policy Management in Patronum+ consists of Allow Domain List and Workflows.

### 6.1 Allow Domain List

This defines domain-based restrictions in workflows, allowing for specific domains to be individually included or excluded. Trusted external Google Workspace domains can be included in file policies. External users from these domains will not be included in file searches.

### 6.2 Workflow

A workflow is a structured sequence of steps that guide policy creation, review, approval, implementation, and maintenance. It ensures consistency and alignment with organisational goals.

#### Scope

These specify which users and drives / files that apply to the policy.

Users in Organisational Units or groups

- All of domain (default)
- Include OU list
- Exclude OU list
- Include group list
- Exclude group list

Files and Shared Drives

- All files in domain (default)
- Users My Drive files
- Include Shared Drive list
- Exclude Shared Drive list

#### Conditions

These specify the events and corresponding filters that trigger the policy.

Attributes

- Document Title
- File type
- Labels
- Modified

- Older than
- Shared
- Shared With
- Shared with domain

#### Values

- Any domain outside allowlist
- Any external domains
- Anyone at domain with link
- Anyone at target audience with the link
- Anyone with the link
- Gmail.com

## Actions

These specify what happens when the policy is triggered.

#### Attributes

- Email to Drive Managers/Content Managers (set frequency of days, months, years)
- Email User (set frequency of days, months, years)
- Expire Files (on specified date)
- Labels (applies labels to targeted files)
- Move Files
- Move To
- Notify
- Report
- SafeList-Days Ago
- Schedule
- Snooze-Days Ago
- Unshare Files