Regulatory & Compliance

How We Handle Your Data

Document Information

Code:	**CD-HWHYD**	Created by:	**Steve Dodson**
Version:	**2.1**	Approved by:	**Lars Sneftrup Pedersen**
Date:	**26 September 2025**	Confidentiality:	**Public**

Admin By Request
ZERO TRUST PLATFORM

Copyright © 2025 Admin By Request

San Francisco, Florida
Wisconsin, New York
(+1) 262 299 4600

Denmark, Norway,
Germany, Benelux
(+45) 55 55 36 57

United Kingdom, Spain
Switzerland, France
(+44) 20 3808 8747

Sweden, Thailand
Finland, New Zealand
(+46) 31 713 54 04

sales@adminbyrequest.com | support@adminbyrequest.com | www.adminbyrequest.com

Table of Contents

1 Introduction

1.1 Purpose

This document explains how Admin By Request (ABR) handles customer data. ABR is a Software as a Service (SaaS) platform for Privileged Access Management (PAM) that allows organizations to remove permanent local admin rights while still enabling users to perform administrative tasks.

1.2 Scope

This document applies to all paying customers subscribed to the ABR SaaS platform. It covers where data is stored, how it is collected, the security mechanisms in place, and the compliance measures to which ABR adheres.

1.3 Audience

This document is intended for:

- Customers with an active subscription
- Internal ABR support and service delivery teams
- Auditors and procurement teams evaluating vendor support obligations

1.4 Related Documents

This document may refer to, and should be read in conjunction with, the following:

- Commitments and responsibilities in ABR's Data Processing Agreement
- Support provisions in ABR's Terms and Conditions and Customer Support Services
- Collection, use and disclosure of personal data in ABR's Privacy Policy and Data Privacy Settings

Refer also to ABR's Trust Center documents.

This document is available online:

How We Handle Your Data

2 Data Storage

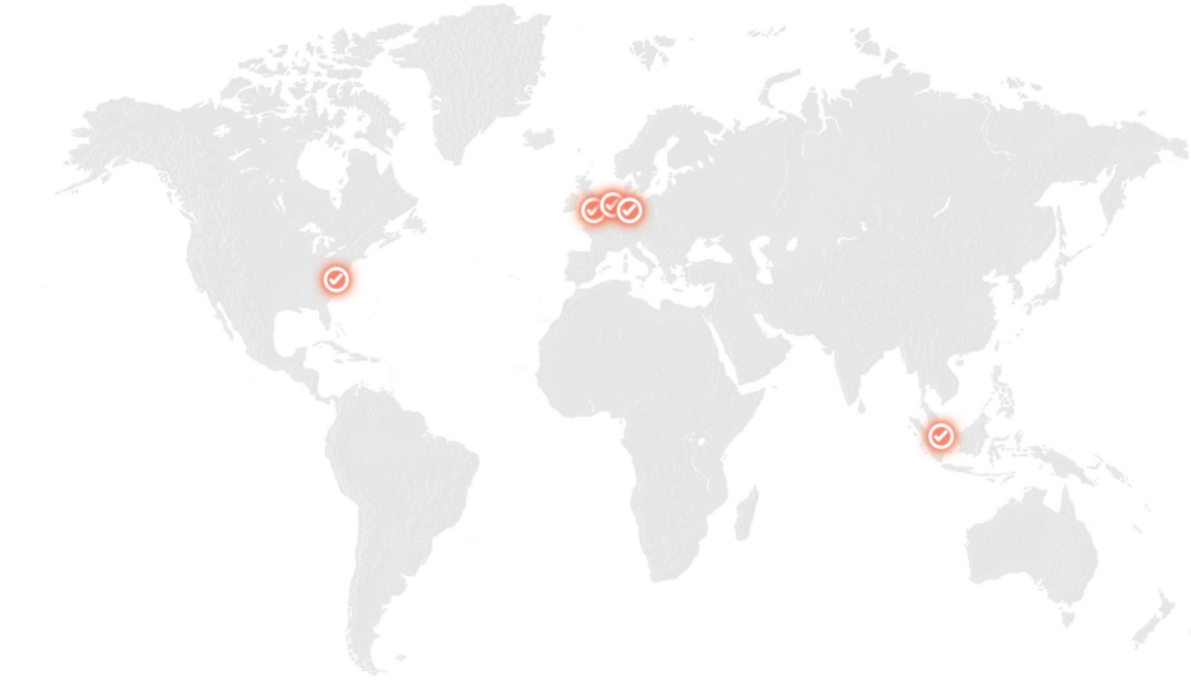
2.1 Where your data is stored

ABR hosts its service entirely in Microsoft Azure. At the time of writing, customer data is stored in Azure SQL databases located in **five** geographic regions. Each region operates a primary and a secondary data center.

Your data is stored in a data center that is located in one of the geographic locations listed below. These are in Europe, the USA, the UK and Asia.

To determine your data location, go to page Tenant Settings > Retention in the portal and note the geographic location shown in field **Data Location**. It will be one of the following:

- **EU West, Netherlands** (Europe - Netherlands)
- **Virginia, United States** (USA)
- **London, United Kingdom** (UK)
- **Frankfurt, Germany** (Europe - Germany)
- **Singapore** (Asia)



By default, ABR uses the region matching the customer's location. However, customers may request storage in another region when licensing the service. No customer data is stored outside these designated regions.

Refer to "Data Collection" on page 4 for regional IP address details.

2.2 Backup and retention

Data is real-time geo-replicated between two locations in each region to ensure backup, fail-over and disaster recovery. Microsoft backs up Azure SQL databases and guarantees an Azure SQL restore is possible from **any minute** of the day, within the last **30 days**. We also do cold storage backups in case of a complete, irrecoverable Microsoft Azure failure on all locations in a region.

Auditlog data is kept for **12 months** by default. Administrators can set the retention period from **three months** to **five years** via portal menu **Settings > Tenant Settings > Retention > DATA RETENTION**.

2.3 Service Level Agreement

Our web servers are located in the same **Azure Availability Set** in each continent.

An Azure Availability Set is a guarantee that Microsoft will not take web servers down for maintenance at the same time. Microsoft guarantees a **99.95%** up time in each continent under this arrangement.

Refer to Service Level Agreements (SLA) for Online Services for more information on Microsoft's commitment to its customers.

For more information on our commitment to you, refer to:

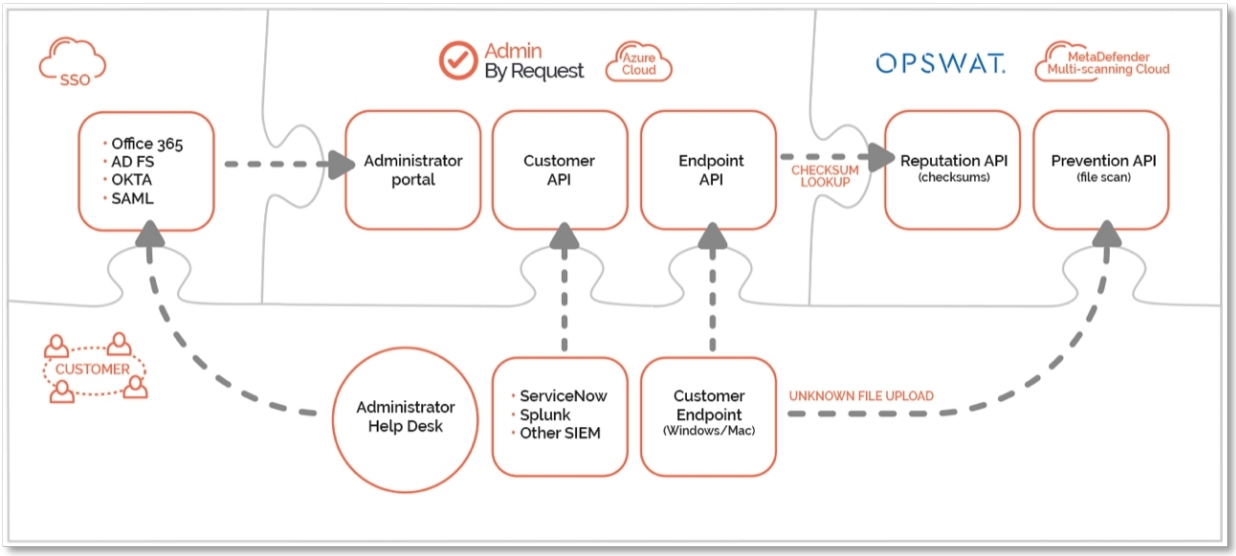
- Data Processing Agreement (Annex III: Technical and Organisational Measures)
- Terms & Conditions (6. Service Level)

3 Data Collection

3.1 Data flow inside the system

The following communications take place:

- The client software communicates with the cloud service
- Administrators and help desk personnel access the portal through single sign-on
- OPTIONAL: Files and checksums are sent to OPSWAT MetaDefender for multi-engine malware scan (**enabled** by default)
- OPTIONAL: Customer API can be used to consume data from your own systems (**disabled** by default)



3.2 Encryption

3.2.1 Encryption at rest

We use Azure SQL transparent data encryption for all data at rest to ensure no unauthorized access to data is possible.

3.2.2 Encryption in transit

The data communication between the client software and our servers uses TLS 1.2 encryption. The load balancer IP depends on your region - refer to the list below.

Admin By Request uses port **443** and the IP addresses and API URLs that need access through firewalls are as follows.

If your data is located in Europe (Netherlands):

- IP: **104.45.17.196**
- DNS: **api1.adminbyrequest.com**
- DNS: **macapi1.adminbyrequest.com**
- DNS: **linuxapi1.adminbyrequest.com**

If your data is located in the USA:

- IP: **137.117.73.20**
- DNS: **api2.adminbyrequest.com**
- DNS: **macapi2.adminbyrequest.com**
- DNS: **linuxapi2.adminbyrequest.com**

If your data is located in the UK:

- IP: **85.210.211.164**
- DNS: **api3.adminbyrequest.com**
- DNS: **macapi3.adminbyrequest.com**
- DNS: **linuxapi3.adminbyrequest.com**

If your data is located in Europe (Germany):

- IP: **9.141.94.162**
- DNS: **api4.adminbyrequest.com**
- DNS: **macapi4.adminbyrequest.com**
- DNS: **linuxapi4.adminbyrequest.com**

If your data is located in Asia (Singapore):

- IP: **52.230.54.129**
- DNS: **api6.adminbyrequest.com**
- DNS: **macapi6.adminbyrequest.com**
- DNS: **linuxapi6.adminbyrequest.com**

Wherever you are, you can also use **api.adminbyrequest.com**, but the regional URLs will likely be more responsive.

3.3 What data does the inventory collect?

You are in control of your data. We offer the option to further limit the collection and processing of certain categories of personal information, or to disable the entire inventory. Once logged-in to the portal, these preferences can be updated at any time in the portal **Settings** menu according to your needs.

Refer to Data Privacy Settings for more information.

3.4 What data is extracted from domain controllers?

The client software collects this information from a domain controller for domain computers:

- User and computer OU names
- User's phone number and email address
- List of computer and user groups

The traffic is marginal and refreshed **every 4 hours** only. You can monitor the traffic on an endpoint by running the ADInsight SysInternals tool.

3.5 Session data collected

When a user has completed an App Elevation (*Run As Admin*) or an *Admin Session*, the client collects:

- Computer name
- Session duration
- Installed and uninstalled software
- UAC elevated programs
- Reason for administrator need (if configured)
- User's account name and full name (if configured)

If the *Reason* screen is used, email address and phone number are also collected, as entered by the user in the pop-up window. As mentioned earlier in this document, you can disable collection of user name, email address and phone number in portal **Settings**.

3.6 Diagnostics data collected

In a support situation, one of our support engineers might ask the end user to invoke the endpoint **Admin By Request About** screen, click the **Diagnostics** button and ask the end user to click **Submit**. This action sends trivial system data to us to understand the history of the endpoint software.

If the end user clicks **Submit**, the client submits:

- Current configuration state (downloaded settings)
- Data in queue to be uploaded
- When the endpoint software was installed or upgraded
- When the services of the endpoint software were started or stopped
- Events from the local event log related to Admin By Request.

NOTE

- Data cannot be extracted by us without the user clicking the **Submit** button.
- Submitted data is kept for a limited time only - typically one week, although longer if a support ticket requires more time to resolve.
- An end user cannot create a support ticket - only your portal administrators can do this.

3.7 Data cached on the endpoint

The client software for domain joined computers works exactly the same off your LAN as it does on your LAN.

This is possible because the endpoint clients cache an encrypted copy of domain groups' names and OU name of the computer and the logged-on user, in order to determine sub settings both online and offline:

- If your computers are Azure AD joined, a similar group cache is kept for performance reasons.
- If your computers are stand-alone, no data is cached.

4 Data Security

4.1 Access to your production environment

Apart from yourselves, only the appointed Risk Owner and/or Asset Owner has access to the production environment (**maximum 2 persons**). Please refer to our Data Processing Agreement for more information.

4.2 Internal security

We have strict security policies in place for all our employees. The Data Processing Agreement (Annex III: Technical and Organisational Measures) contains more information on the steps we take to protect your data.

We have been audited and are certified in a number of areas, including **ISO 27001**, **Cyber Essentials Plus** and several **independent pentests** - please refer to the Trust Center for full details.

Don't hesitate to contact us if you have any questions about data security at Admin By Request.

4.3 Malware-free updates

In addition to using OPSWAT MetaDefender, we use **VirusTotal Monitor** (VT monitor) from VirusTotal to ensure Admin By Request updates are free of viruses and other malware.

VirusTotal is owned by Google and offers scanning of files from **over 70 antivirus scanners and URL/domain blocklisting services**, including well-known brands such as Avast, Avira, Bitdefender, Kaspersky, McAfee, Sophos, and Trend Micro, as well as specialized security vendors like Cylance, DeepInstinct, CrowdStrike, and SentinelOne.

When we release updates, the binary files are uploaded to our VT monitor account for inspection and we thereby have confirmation that the files are clean before we put them into production for you to download.

Should any files be flagged as false positives by a vendor, this vendor is automatically notified and we await resolution before releasing the code. Proactively, we also keep the last three releases in our VT monitor account. All files are then scanned every day by all 70+ engines. We are notified if any false positives arise and we make sure the vendor flagging the file adds it to their approval list for future reference.

> The key takeaway is that our files simply cannot be deployed without passing the scan of all 70+ engines.

Refer to How it works for more details on VirusTotal's scanning and inspection process.

5 Compliance

5.1 Terms & Conditions

Together with the **Data Processing Agreement** (see below), our **Terms & Conditions** are the legal artifacts that govern your use of Admin By Request.

> Refer to Terms & Conditions for the full text of this agreement.

5.2 Data Processing Agreement

Admin By Request is a European company, and we must therefore abide by the EU **General Data Protection Regulation (GDPR)**.

To comply with Article 28 in the GDPR, any European company must provide a **Data Processing Agreement (DPA)** between themselves and any European customer. The agreement applies to all customers around the world, which means all customers reap the benefits of the GDPR requirements observed by us.

The overall purpose of Article 28 is to describe internal procedures relating to security, availability and privacy when managing customer data, with the main objective being customer transparency.

> Refer to Data Processing Agreement for the full text of this agreement.

5.3 ISO 27001

ISO/IEC 27001 is an information security standard - part of the ISO/IEC 27000 family of standards. It is published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) under the joint ISO and IEC subcommittee.

ISO/IEC 27001 specifies a management system that outlines security requirements and is intended to bring information security under management control. Organizations that meet the requirements may be certified by an accredited certification body following successful completion of an audit.

> Admin By Request is **ISO 27001** certified. Download this certificate in the Trust Center.

Refer to ISO/IEC 27001:2022 for further details on this certification.

5.4 SOC 2

Service Organization Control 2, known as SOC 2, is developed by the American Institute of CPAs (AICPA) and defines the criteria for managing customer data based on five "trust service principles":

1. Security
2. Availability
3. Processing Integrity
4. Confidentiality
5. Privacy

SOC 2 and GDPR Data Processing Agreements are very similar and they both address the same procedures. The key difference is that a GDPR Data Processing Agreement is based on the right to audit by the customer, whereas SOC 2 is a certification by a trusted third party.

> The **SOC 2 Type 2** report issued for Admin By Request by the C3PAO, A-LIGN, can be downloaded in the Trust Center.

Refer to AICPA-CIMA for further details on this certification.

5.5 Cyber Essentials Plus

Cyber Essentials and **Cyber Essentials Plus** are the UK Government's answer to a safer internet space for organisations of all sizes, across all sectors.

Developed and operated by the National Cyber Security Centre (NCSC), Cyber Essentials is considered the best first step to a more secure network, protecting you from 80% of the most basic cyber security breaches.

> In addition to Cyber Essentials, Admin By Request complies with the requirements of the **Cyber Essentials Plus** scheme. The certificate can be downloaded in the Trust Center.

Refer to Cyber Essentials for further details on this certification.

6 Tenancy

6.1 About multitenancy

The service we provide to you uses a **multitenancy** model. Multitenancy is the norm for Software as a Service (SaaS) solutions and is the model used by all major SaaS solutions, such as SalesForce or Google Apps – and also your bank.

Your bank does not have a separate system for you as a customer, instead your bank uses multitenancy, which means that a set of pooled computing resources is shared among multiple customers (tenants) using application level isolation. A tenant (e.g. your company as a customer in your bank) is a group of users who share a common access with specific privileges to the software instance.

With a multitenant architecture, the software application is designed to provide every tenant a dedicated share of the instance - including its data, configuration, user management and individual functionality.

Please refer to the Microsoft tenancy design pattern page for a deeper explanation of **SaaS and Multitenancy**.

7 Portal

7.1 Access

At the time of licensing, you will receive a main login. From this main login, you can create multiple additional logins with limited access, such as access for an auditor or a manager. A login also grants rights to see the same data in the mobile app.

For all users, you can enable two factor authentication and single sign-on.

If you received an NFR license for a proof-of-concept project, and you later choose to license, this tenant instance will automatically roll on to become your commercially licensed tenant.

7.2 Single sign-on

We support single sign-on (SSO) for Office 365, Azure AD, ADFS, Okta and any SAML 2.0 identity provider. We recommend that you set up single sign-on because this ensures that you terminate access to the portal when employees leave the company.

> Refer to Single Sign-on Setup for technical setup of SSO.

7.3 Availability

As described in "Data Storage" on page 2, we use Azure web servers in multiple continents in order to make sure we provide great performance anywhere in the world and that the portal is always up and running.

7.4 Denial of Service Protection

The portal is protected from Distributed Denial of Service (DDoS) attacks by Microsoft's **Azure DDoS Protection**.

> Refer to What is Azure DDoS Protection? for more information.

8 Document History

Version	Author	Changes
20 March 2024 **1.3**	J. B. Sorensen	Annual review.
20 August 2025 **2.0**	Steve Dodson	Annual review. Updated manual structure and layout, aligned with Terms & Conditions, Data Processing Agreement and other documents. Added information about additional global data centers.
26 September 2025 **2.1**	Steve Dodson	Removed out-of-date reference to Internal Security Policy and added links to Data Processing Agreement (Annex III) and Trust Center in chapter "Data Security". Added Cyber Essentials Plus certification in chapter "Compliance".