Bundledocs

Security FAQ

Let's get started…

bundledocs

BACKGROUND INFORMATION	
Company name	Meditati Limited (Bundledocs)
Registered Address	Westpoint Business Campus, Link Road, Ballincollig, Cork P31 E446, Ireland
Contact details	infosec@bundledocs.com
REGULATORY	
What accreditations is your company registered with?	We have completed the ISO 27001 certification process.
Do you have a GDPR programme in place?	You can find more information on our GDPR compliance below. https://www.bundledocs.com/privacy-policy
Do you have a Data Protection Officer?	You can reach Bundledocs' appointed Data Protection Officer (DPO) via email at dpo@bundledocs.com
Do you have a security policy?	You can find more information on security at Bundledocs below. https://www.bundledocs.com/security
Do you have a data protection policy to cover personal data?	You can find more information on our data protection policy below. https://www.bundledocs.com/privacy-policy
Do you have a formal procedure for reporting data leaks/breaches, including suspected data leaks/breaches, within 72 hours?	After an incident has occurred a root cause analysis is carried out which may result in recommendations for changes to policies or procedures. These recommendations will then be reviewed by CTO and implemented where necessary. Every effort will be made to notify clients of any security incident once it has been mitigated to avoid exploitation of the incident.

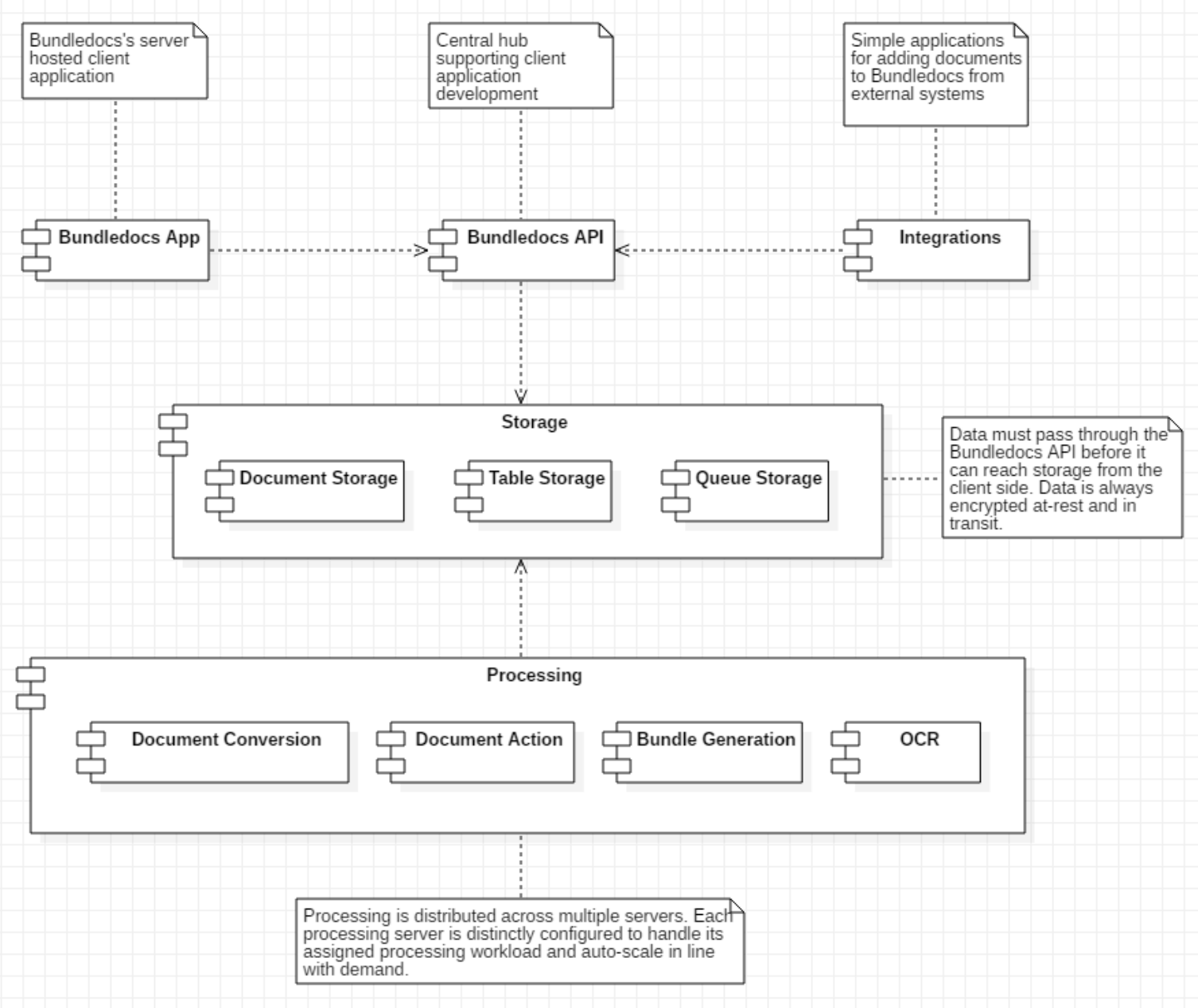
	We comply with the following breach notification guidelines which include a clause on notifying affected parties within 72 hours of a breach. https://www.dataprotection.ie/en/organisations/know-your-obligations/breach-notification
Describe your data security training for employees.	We conduct security awareness training to which all staff must acknowledge and adhere to. We follow OWASP principles to ensure a high degree of security awareness during development. All development staff are required to attend at least one instructor led security awareness training course each year.
DATA PROCESSING & FLOWS	
Please provide a description of the data processing / services provided by your company for the Customer	Bundledocs software allows users to swiftly and easily compile document bundles for a number of purposes including court bundles, deal bibles, transaction bibles, e-briefs and report books.
What is the volume of Customer data processed by you? Please indicate whether pm/pa.	This is determined by the Customer.
Please indicate the categories of data collected, processed and shared by you (on behalf of Customer only). Delete as appropriate.	All Bundledocs data is classified as highly sensitive.
Please describe the data processed	Any documents and metadata supplied by Customer.
What categories of data subjects are processed as they relate to the services you provide to Customer?	Any documents and metadata supplied by Customer.
Please describe how the personal data is received and subsequently moves through your company. Include systems used, formats of data and people involved at all touch points of the personal data flow.	All Customer data is sent directly to the Bundledocs service hosted in Microsoft's Azure Cloud over a secure TLS 1.2 connection or above. The data is transformed into a single PDF document automatically by one of our Microsoft managed servers at the request of the Customer. This happens automatically within Microsoft's Azure Cloud data centre.

	When a Customer downloads the result of this processing the new document is transmitted directly from Microsoft's Azure Cloud data centre to the user over a secure TLS 1.2 connection or above. At no point in this process are Bundledocs staff privy to the contents of those documents provided by Customer or produced by Bundledocs. *A supporting system architecture diagram has been appended for clarity.*
How do you store and secure the personal data within your business? List different methods – systems, anonymization, encrypting, masking, passwords, restricted user access, segregation from other Client data etc	All Customer data is encrypted at-rest within Microsoft's Azure data centre. In Bundledocs, each user is logically segregated from all other users and all data is encrypted at-rest.
In what format(s) is the personal data stored? E.g. data files, audio, image, paper	Typically, Bundledocs users provide standard office documents and related metadata.
Who has access to the personal data? How do you monitor and control access to the personal data?	Access to Customer data is highly restricted to key personnel only and restricted to a restricted set of metadata only. We use Azure Monitor for monitoring and Azure Active Directory supported by two-factor authentication to control access.
Do you process/use the data in any way other than for the purpose specified by Customer?	No
Do you back up the personal data? Where is this stored (include locations of server if applicable)?	All Bundledocs data is backed up at regular intervals. These backups are stored under the same conditions as our production data. At no point does any Customer data contained within our backups leave Microsoft's Azure Cloud data centres. Customer data may persist in our backups for up to seven days.
How is data deleted (both paper and electronic)?	Paper data is destroyed using a cross shredder. Electronic data is destroyed using a secure media destruction system. Upon a system's end-of-life, operational personnel follow rigorous data handling and hardware disposal procedures to assure that hardware containing data is not made available to untrusted parties. We use a secure erase approach for hard drives that support it. For hard drives that can't be wiped, we use a destruction process that destroys

	the drive and renders the recovery of information impossible. This destruction process can be to disintegrate, shred, pulverize, or incinerate. We determine the means of disposal according to the asset type.
What is your retention and deletion policy / guidelines for storing the personal data?	Customer users are responsible for removing data from the platform.
Will your organisation be able to handle instances when we request personal data be deleted from your system(s) where appropriate to?	The removal of specific content is the responsibility of the owner of the content. We may remove all data owned by specific Customer users if requested to do so.
Describe your method(s) for restricting the processing of personal data on request.	Access can be revoked for specific Customer users to prevent further processing of personal data owned by those Customer users. We are happy to discuss any further measures that may be necessary which may include purging specific Customer users.
Has your company or any directors been subject to any regulator investigation or disciplinary action for a personal data breach?	No
Provide total number of **suspected** personal data security breaches in the past 12 months.	Zero
Provide number of **actual** personal data security breaches in the past 12 months.	Zero
Please provide a copy of each relevant mechanism for providing the lawful basis for processing Customer data.	https://www.bundledocs.com/terms-of-service https://www.bundledocs.com/privacy-policy/ https://www.bundledocs.com/security
DATA SHARING	
Is the data shared with a third party (including for administration, support, reporting or otherwise?)	Yes, Microsoft Azure: Cloud Computing Services

If yes, please provide details on who the third parties are, what processing is conducted by the third parties and why.	At Bundledocs, we use Microsoft' Azure Public Cloud platform to deliver our service. We use the "Azure Cloud Services" platform which means Microsoft are responsible for the management of the network layer of our application. https://azure.microsoft.com/en-us/overview/what-is-paas/ We provide configuration files that describe the size and number of VMs that we need for a particular workload and Azure handles the provisioning and management of the resources required to provide the configuration. https://docs.microsoft.com/en-us/azure/cloud-services/cloud-services-choose-me
Where is the third party located?	Bundledocs' data is stored in Europe by default, in Microsoft's Azure Cloud data centres in Dublin, Ireland and Amsterdam, Netherlands. Bundledocs is a true cloud-based solution and as such data may be retrieved from either European location during disaster recovery or redundancy scenarios. Customer may choose to store their documents in United Kingdom, in Microsoft's Azure Cloud data centres in London, England and Cardiff, Wales. Bundledocs is a true cloud-based solution and as such data may be retrieved from either United Kingdom location during disaster recovery or redundancy scenarios. Customer may choose to store their documents in Australia, in Microsoft's Azure Cloud data centres in Sydney, New South Wales and Melbourne, Victoria. Bundledocs is a true cloud-based solution and as such data may be retrieved from either Australian location during disaster recovery or redundancy scenarios. Customer may choose to store their documents in the United States, in Microsoft's Azure Cloud data centres in Virginia East US and Virginia East US2. Bundledocs is a true cloud-based solution and as such data may be retrieved from either Australian location during disaster recovery or redundancy scenarios.
How is the data protected in transit?	Bundledocs uses TLS 1.2 encryption technology or above to ensure a secure channel of communication between our servers and the user's browser.

	Any communication between our web servers and operational services such as our data storage service or document processing service is secured in this way. This ensures that at no point can Bundledocs data be deciphered during any routing operations.
How is the data protected in the hands of the third party?	Microsoft do not have access to any Bundledocs data in an unencrypted form.
Do you monitor the use of the data in the hands of the third party?	Microsoft do not directly handle Bundledocs data but instead provide services on which the Bundledocs service may operate.
Are you conducting reviews with these third parties to ensure their GDPR compliance?	Microsoft are fully GDPR compliant, you can find more information on GDPR at Microsoft below. https://docs.microsoft.com/en-ie/legal/gdpr
Describe how the personal data is transferred / shared with these third parties	Customer personal data is not shared directly with Microsoft, rather, all Bundledocs data and services reside securely in Microsoft's Azure Cloud data centres.
Describe methods / tools used to secure the personal data in transit.	Bundledocs uses TLS 1.2 encryption technology or above to ensure a secure channel of communication between our servers and the user's browser.
Do you transfer personal data for any reason outside of the EEA?	No
Any other comments?	
	The below diagram shows the directionality of data as it flows through the various Bundledocs components. In Bundledocs, each user is logically segregated from all other users. A user's bundle can only be made available to another user through an explicit action undertaken by that user or their organization administrator.


Bundledocs's server hosted client application
Central hub supporting client application development
Simple applications for adding documents to Bundledocs from external systems
Bundledocs App
Bundledocs API
Integrations
Storage
Document Storage
Table Storage
Queue Storage
Data must pass through the Bundledocs API before it can reach storage from the client side. Data is always encrypted at-rest and in transit.
Processing
Document Conversion
Document Action
Bundle Generation
OCR
Processing is distributed across multiple servers. Each processing server is distinctly configured to handle its assigned processing workload and auto-scale in line with demand.

Contact the Bundledocs Team Today!

Any Questions? We endeavor to help you with any queries or issues you may have. Get in touch with the Bundledocs team today. We're here to help!

CONTACT

Call: +353 (0)21 4826320
Email: info@bundledocs.com
Web: www.bundledocs.com

Postal Address:
Westpoint Business Campus,
Link Road,
Ballincollig,
Co. Cork,
Ireland