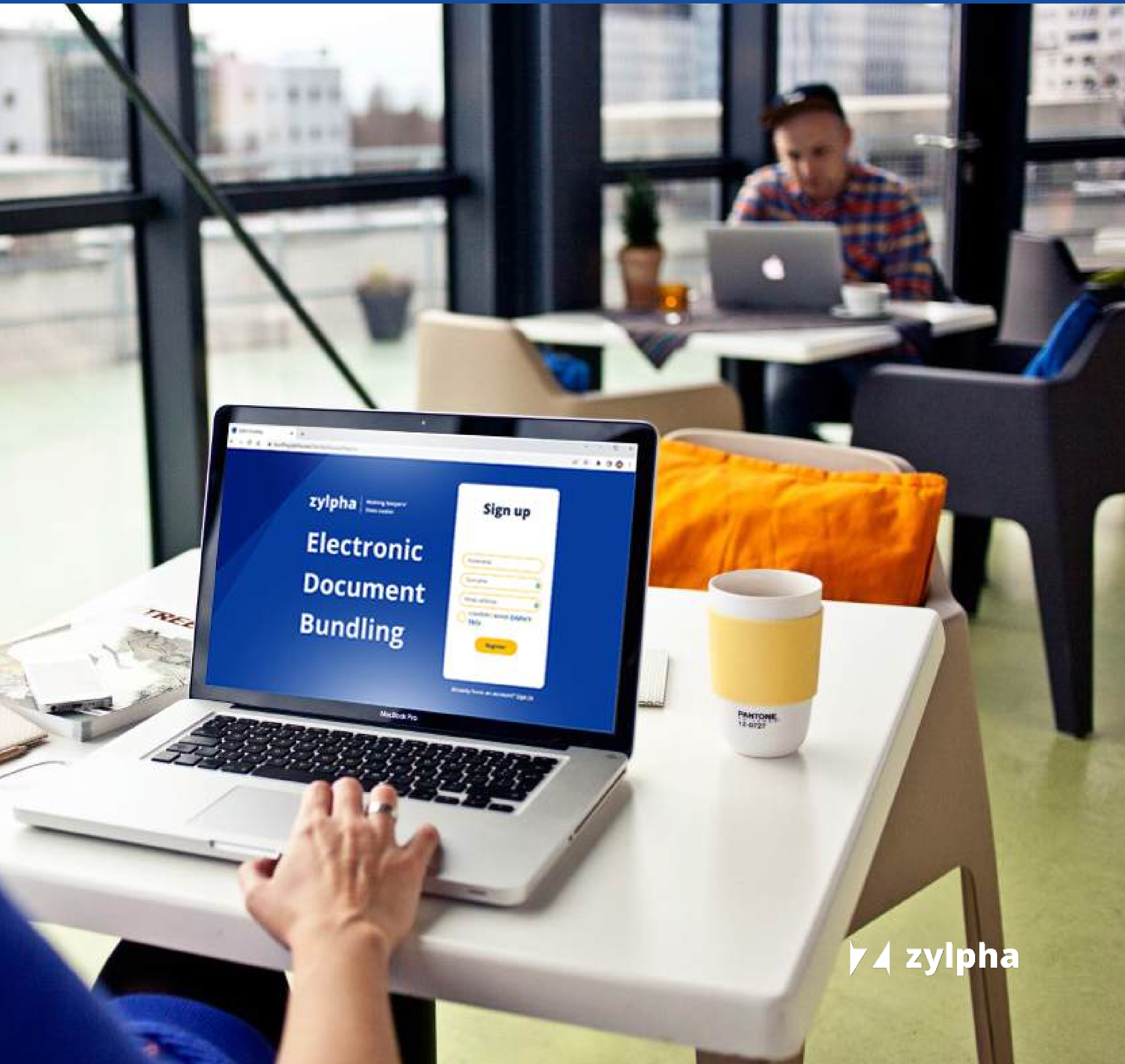
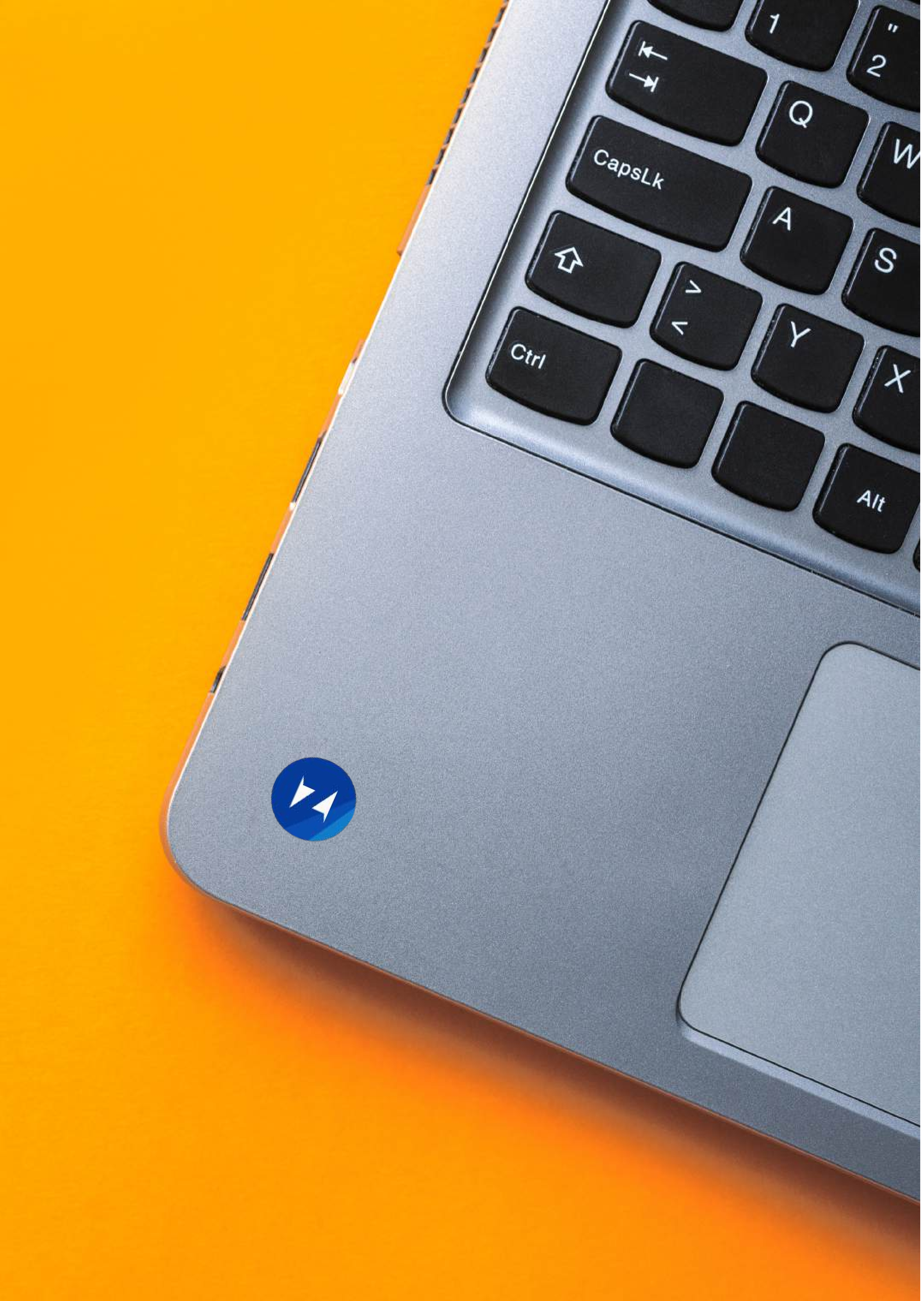
Online Bundling
Data Security



zylpha



Data Center Security

As a company that takes data security and privacy very seriously, we recognise that Zylpha's data security practices are important to you. While we don't like to expose too much detail around our practices (as it can empower the very people, we are protecting ourselves against), we have provided some general information to give you confidence in how we secure the data entrusted to us.

Zylpha Online Bundling is built on Azure App Services with the inbuilt security that Microsoft provides. For more information on Azure App Services see this link: https://learn.microsoft.com/en-us/azure/app-service/overview-security

The App Services use Azure zonal redundancy to ensure a highly durable service. The services are synchronized across 3 zones (each zone being one or more data centres) in the Azure UK South region. This applies to both the web services and the document storage. The document storage is also copied to the Azure UK West region, keeping all data under the England and Wales jurisdiction.

Protection from Data Loss, Corruption

As the documents stored are copies of the local source documents, there is currently no restore option provided to end users in the event of accidental deletion.

The Azure databases used by the application are not accessible via public endpoints. Access is via private virtual network. Data is encrypted at rest and backed up automatically.

Application-Level Security

As the service stores the converted documents used in the bundles, the storage of the document data is of critical importance. The document storage has the following security and backup configuration:

- The Zylpha Online Bundling services use an Azure storage account that can only be accessed by the application in a backend Azure virtual network.
- There are 2 layers of encryption at rest, one at the Microsoft Service level, and one at the Zylpha infrastructure level, with two different encryption algorithms and two different keys providing exceptional protection against data breaches and other threats.
- Azure role-based access controls are used to restrict access to the storage at control level only, so no developers or administrators have access to the users' documents.
- Each bundle is stored in its own Azure storage container, only accessible to the end user.
- Operational backup is enabled for a continuous backup solution. Note that this is not a backup service for Zylpha Online Bundling users.

Other application security features include:

- The all data in transit is encrypted with TLS 1.2 or higher.
- Login pages have brute force protection.
- We arrange regular external security penetration tests which are carried out by security experts.

Internal IT Security

- Zylpha employs the highest-level security features available in Microsoft 365 to monitor and, in most cases, automatically resolve issues.
- Zylpha employs the latest Microsoft zero-trust identity boundary policies to our networking.
- Multifactor authentication is activated on Microsoft 365 for all users and requires two additional forms of authentication to verify a password change.
- Network architecture is optimised to provide a high level of protection against ransomware.
- We have a team that monitors our environment for vulnerabilities. They coordinate penetration testing and social engineering exercises on our environment and our employees.
- Zylpha employs password management software, deployed to all internal users, to monitor use of, and strength of, passwords for all internal and 3rd party online supplier services. The software also monitors the dark web for breaches and activity associated with all credentials stored by each user.
- Multifactor authentication is activated on all 3rd party online supplier services where available. Non availability of MFA on services would rule out the use of that service on accounts where the security was assessed as a requirement.
- All software and online services are approved and managed as part of our Information Security Management System (see ISO 27001 certification).

Protocol & Education

- We continuously train employees on best security practices, including how to identify social engineering, phishing scams, and hackers. This training must be completed for every new employee as part of their probation, and all employees must complete the training every two years.
- Client contact data is stored in our CRM System. All user accounts have MFA enabled as standard and our CRM is now part of our Azure Active Directory (AAD).
- Employees on teams that have access to customer data (such as tech support and our engineers) and background checks prior to employment.
- All employees clearly understand their responsibility in protecting customer data as part of their induction process and regular training.

ISO 27001 Certification

The International Organization for Standardization 27001 Standard (ISO 27001) is an information security standard that ensures office sites, development centres, support centres, and data centres are securely managed. These certifications run for 3 years (renewal audits) and have annual touchpoint audits (surveillance audits).

Zylpha follows a constantly reviewed and improved information security policy and is certified to ISO 27001. Our certification number is: GB22/00000243.

Protecting Ourselves Against You

Yes, you heard that correctly. We can secure ourselves like Fort Knox, but if your computer gets compromised and someone gets into your Zylpha account, that's not good for either of us.

- We monitor and will automatically suspend accounts for signs of irregular or suspicious login activity.
- Certain changes to your account, such as to your password, will trigger email notifications to the account owner.
- Accounts not verified within 30 days are deleted.
- Accounts (not on a paid plan) are deactivated after 30 days of inactivity and deleted after a further 30 days has elapsed.
- We make 2-Factor Authentication available to our customers.

Investing in your privacy

Our products are designed with a 'privacy first' mindset and train our developers and engineers to make sure our products and features comply with UK laws.

Office Hours

9.00am - 5.30pm Monday to Friday (excluding Public Holidays in England)

+44 1962 658 881

Technical Support
support@zylpha.com

General Enquiries
hello@zylpha.com

zylpha

Grosvenor House, 2 Grosvenor Square, Southampton, Hampshire SO15 2BE
01962 658 881 **hello@zylpha.com** **www.zylpha.com**