

Cloud computing adoption FAQs (May 2020)

Introduction

Thank you for taking the time to find out more about Hymans Robertson's continued adoption of cloud computing.

This document provides detailed information and links to other resources, which we hope you'll find useful.

If you would like more information or have any questions, please don't hesitate to get in touch with your Hymans Robertson consultant in the first instance.

Why we're adopting cloud computing

1. What is the cloud?

A common definition of the cloud is "a network of remote servers hosted on the internet and used to store, manage, and process data in place of local servers or personal computers". Typically large-scale computing resources are provided by cloud computing vendors from secure data centres.

2. Why are you using cloud computing?

Cloud computing provides the following benefits:

- **Security:** We think that the cloud is the most secure place to store data and run applications. The cloud's industrial-grade infrastructure plays an important role in addressing cyber security risks, for example.
- **Scalability:** The cloud provides the scalability to meet increasing demands from our clients by allowing us to dynamically increase compute power and storage capacity.
- **Agility:** The cloud helps us to shorten the development lifecycle, enabling us to better meet the evolving needs of our clients by delivering new applications and services more quickly.
- **Innovation:** Being on the cloud opens up access to a range of new technologies like AI and machine learning – technologies we wouldn't otherwise be able to take advantage of.

All of this means we will be positioned to deliver a better service to our clients and develop and deploy new applications and services more quickly and efficiently.

3. Is this in line with market practice?

Yes. Our research shows that many firms in the financial services sector – including our competitors – are using cloud computing to some extent. Many of our clients are actively using the cloud too.

Our cloud computing partner: Microsoft

4. Why have you chosen Microsoft?

We've chosen Microsoft as our cloud computing partner for a number of reasons, including:

- We're already aligned to Microsoft's product and technology set (for example Microsoft Office applications).
- Microsoft has demonstrated a firm commitment to compliance, for example with global standards including ISO27001 and EU model clauses for GDPR compliance.
- We have choice and control over where applications are run, where data is stored and who has access to it – in particular, we will only use data centres located in the European Economic Area (EEA).

5. What cloud services are you using?

We're using Microsoft Azure Cloud Services to develop, package and deploy applications and services to the cloud. We will also use Microsoft Dynamics and Microsoft Office 365 to run Office applications, including email.

6. Where are Microsoft's data centres located?

We're currently using Microsoft's data centres located in UK, Dublin and Amsterdam.

7. What agreements do you have in place with Microsoft?

We have negotiated an English-law commercial contract with Microsoft Ireland Operations Limited. It includes Microsoft's Online Services Terms, which govern the provision of cloud services. The Online Services Terms include terms and conditions that comply with Article 28 of the GDPR and they also incorporate EU model clauses. Microsoft's cloud services are backed by a comprehensive Service Level Agreement.

8. What due diligence have you carried out?

We've had a good working relationship with Microsoft at both an account and technical level for several years. Since Azure adheres to many of the [international and industry-specific compliance standards](#), our robust due diligence checks are made easier. We've also been fortunate enough to get a tour of the Dublin data centre – and were thoroughly impressed by its scale and sophistication.

How we're making the transition to cloud computing

9. What are you moving to the cloud – and when?

For brand new propositions, we'll adopt a "cloud first" approach, meaning that we'll build and deploy new applications using Microsoft Azure. We'll move existing systems, applications and services to the cloud where there's a clear benefit in doing so, for example to make things more secure, to upscale our capabilities or to take advantage of new technologies or innovations only available on the cloud. This will take place gradually, on a case-by-case basis.

10. What about systems from other vendors?

We use a number of proprietary systems which are currently all deployed on-premise. We've moved our HR system to the cloud and our finance systems is being moved to the cloud later this year. We don't have any plans to move other systems to the cloud at the moment but will keep this under review.

What cloud computing means for you

11. Will I notice any change in my services?

Our services will continue to operate as usual. When we move services to the cloud, you won't notice any difference in appearance or experience any degradation in functionality. Service levels and usage limits we've agreed with you will remain the same and your usual point of contact remains the same.

12. Will I need any special software or equipment?

No. You'll continue to access applications using standard web browsers and web service protocols for APIs.

13. What about availability?

The target availability of the Microsoft Azure infrastructure is 99.95% excluding planned outages, and this is backed by our contractual agreement with Microsoft. This compares well against the rest of the cloud service market and means we can continue to deliver reliable applications and services with confidence.

About security

14. Is Microsoft Azure secure?

Microsoft Azure is ISO27001 certified and meets the security, privacy, compliance and risk management requirements as defined in the ISO/IEC 27002 code of best practices for information security management and

the Cloud Security Alliance Cloud Control Matrix. For comprehensive information about security, visit the [Microsoft Azure Trust Centre](#).

15. Who has access to data stored in the cloud?

Only Hymans Robertson client-servicing staff are authorised to access client data. Staff are assigned a unique set of access privileges that allow them to access or modify data as required for their job function. Microsoft don't have access to data we store in the cloud, unless we give them permission to do so as part of helping us to troubleshoot a specific issue. In this situation, access will be granted for a named individual to a narrow set of resources relevant to the problem and for a limited time window. To date, we have not had cause to invoke this. No one else has access to data stored in the cloud.

16. Is data encrypted in the cloud?

Yes. Data is encrypted both "at rest" (where it resides on servers in Microsoft's data centres) and "in transit" (when it is transmitted to and from Microsoft's data centres).

17. Has penetration testing been carried out?

We're committed to performing annual penetration testing of all our external-facing applications – whether they are on premise or on the cloud. On request, we can provide clients with a letter from our test partner confirming the date of testing and sites tested. Microsoft conducts its own penetration testing in accordance with ISO27001 and other industry standards.

18. What access logs are kept?

All of our platforms are subject to both infrastructure- and application-level logging. Logs are monitored to identify unusual behaviour, triggering investigation and where necessary specific action. End users may be able to see some elements of their log, for example the date and time of their last log on. Otherwise log files will be strictly controlled and only accessible to administrators with appropriate privileges.

19. How is data backed-up?

Data is backed up in real time in triplicate on Azure to prevent loss of data due to hardware failure and. Azure backups are configured to allow point in time recovery where required. Backups are contained within the Microsoft Azure environment using secondary data centres we've selected (for example, data in the Dublin data centre might be backed up to Amsterdam). No backups will be made to media such as tape and stored offsite.

20. How can you be sure data is permanently deleted in line with your contractual commitments?

We remain in control of how and when data is archived and deleted, in line with our data retention policy and contractual commitments to our clients. Microsoft Azure has sophisticated data deletion processes that ensure that once we request that data is deleted, it cannot be recovered by anyone. Furthermore, when the physical media needs to be decommissioned, Microsoft has a strict process for purging or destroying these devices in accordance with NIST 800-88 Guidelines for Media Sanitation.

About data protection and GDPR

21. How do Hymans Robertson and Microsoft comply with GDPR?

We want our clients to have absolute confidence in the way we protect the data that they entrust to us. We've invested heavily in processes, technology, and above all in our people so that we are a centre of excellence in data protection. You can read more about how we've risen to the challenge of GDPR (including information on our data retention policy and information about our sub-processors) on our online Trust Centre here:

<https://www.hymans.co.uk/information/trust-centre/>.

Microsoft also takes data protection compliance seriously, resulting in the [seal of approval from European data protection experts](#). You can read more about Microsoft's approach to GDPR here: <https://www.microsoft.com/en-us/TrustCenter/CloudServices/Azure/GDPR>.

22. Will you conduct a Data Protection Impact Assessment (DPIA)?

Yes. Where required, we will conduct (or update) a DPIA before we move applications and services to the cloud.

23. Will any personal data be transferred outside the European Economic Area?

Under exceptional circumstances, a Microsoft support engineer who has been authorised to access data by Hymans Robertson may be based in a country outside the EEA. Any such access will be tightly controlled. Microsoft has entered into EU-approved contractual clauses, which ensures that any such access is subject to "adequate safeguards" required under the GDPR. We have similar arrangements with our on-premise data centres, where specialist remote support may be required to help us resolve an issue, so the position is no different with the cloud.

24. Will you still be able to assist us with individual rights requests and other obligations under the GDPR?

Yes. Our adoption of cloud computing will not affect the assistance we will provide you with, in line with our contractual obligations to you.

25. What happens if there's a personal data breach?

Microsoft are obliged to notify us of any security incident affecting data we store on the cloud. Information security incidents or data breaches are handled in accordance with our Security Incident Reporting policy. We have established a data breach response team, who are primarily responsible for responding to and managing a serious data breach in line with our Data Breach Response Plan. In the unlikely event of a breach affecting your data, you will be notified in line with the GDPR and our contractual commitments to you.

More information

Hymans Robertson Trust Centre: <https://www.hymans.co.uk/information/trust-centre/>

Microsoft Azure Trust Centre: <https://www.microsoft.com/en-us/TrustCenter/CloudServices/Azure>

The information in this document has been compiled as at 11 May 2020 and is subject to change.