ACT 365 Security Statement

ACT365 is a cloud based access and integrated video management solution. ACT365 is hosted in the Microsoft Azure datacentre in Ireland. The privacy of ACT365 data is extremely important to ACT.

This website is dedicated to earning your trust on the following matters:

- Your data is safe
- Your data privacy is protected
- Your data is stored in Ireland
- Your data is owned and controlled by you

Data Storage

Your data is stored in the Microsoft Azure Datacentre in Dublin, Ireland. This is Microsoft Azures Northern Europe Region Datacentre.

Click here to see a list of all Microsoft Azure Datacentre Regions.

Microsoft Azure complies with EU Data Protection Directive (95/46/EC) which is a directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Your data will be stored in the Irish datacentre and will not be moved from this datacentre unless in an extremely rare circumstance as set out in the directive above.

Data is stored in Microsoft SQL Server, the database is encrypted using Transparent Data Encryption. Databases are backed up several times per day, backups are held off site in case of a catastrophe.

Data Access

ACT engineers do not have default access to ACT365 databases. ACT365 databases can only be accessed from ACT specific and approved IP addresses along with authentication passwords. ACT engineers will only access the ACT365 database for legitimate technical support purposes and then only under Senior Engineer supervision.

Data Ownership

You own your data that you place in your ACT365 system including CCTV footage, employee information, log events such access granted or access denied, time and attendance information. ACT will not use your data or derive information from it. This data is always accessible to you at www.act365.eu using your unique username and password.

Data Security

Microsoft Azure meets a broad set of international and industry-specific compliance standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2, as well as country-specific standards like Australia IRAP, UK G-Cloud, and Singapore MTCS.

Rigorous third-party audits, such as by the British Standards Institute, verify Azure's adherence to the strict security controls these standards mandate.

Learn more about Microsoft Azure compliance here.

In short, you know your data is secure for the following reasons:

1. The data is stored in Microsoft Azure datacentres which prides itself on meeting all of the above data protection and security standards. This includes adhering to all of the necessary physical and network security protocols required.
2. All data moving to and from the datacentre is encrypted (2048 bit SSL).
3. If you want to access the data you have to access it through a https:// URL and the website it password protected.
4. Access to all databases is blocked by default and only whitelisted IP addresses have access, the only IP address with access is the ACT office.

How long is my data stored for?

ACT will store your data for as long as you are using the ACT365 service. If you decide to discontinue with the ACT365 service your data will be deleted from the Azure servers.

Data such as auditing and log events will be removed after a period set out in your agreement (usually 6-12 months).

Security Auditing

ACT routinely engage the services of third party expect in cyber security to fully audit and highlight any security threats. They are given access to the cloud system and the hardware where they will attempt a circumvent security. The system has been fully tested and is fully compliant with the OWASP Top 10 security threats. This gives ACT absolute confidence in the security of our products.

Microsoft continuously monitor for any hint of suspicious activity, so much so that when ACT and our security partners simulate a DDOS attack we need explicit permission from Microsoft for our 'test' to not be flagged as a legitimate attack.

Authentication

Once a user is registered to use the system they must accept an invite via the email address they have signed up for. The system enforces that a user creates a complex password. It is not possible for anybody to ever view a user's password.

The ACT365 portal provides a very granular security model, it is possible to grant permissions ranging from giving full access to a customer user to all that customers site to being able to grant user only read only access to the just a single site. A customer can also disable their installer from accessing any of their data if they so wish.

Interaction with Internal Network

ACT365 ACU and VCU will be installed on the local network. These devices will communicate with the ACT365 cloud service over SSL (TLS.1.2), this communication is only ever on port 443. All traffic is fully encrypted. The messages are sent using the Google Protocol Buffer Specification. All messages must contain valid authentication attributes or will be rejected by the ACT365 server.

There is no need to open any ports other than 443 on your network. There is also no need for port forwarding of any kind.

The ACU and VCU are both configured to use DHCP out of the box so they will function in much the same way as any other IP device on the network. They can also be set to use static IP addresses if required.

Security Protocols

As previously stated all interactions with the ACT365 cloud service is encrypted using TLS 1.2. All messages to the server will also contain encrypted authentication attributes. ACT have enlisted the service of third party security experts to see if they could break any of the security protocols, they couldn't.