access
freedom to do more

Access Group Organisational Security

Document Control Reference: OSD v3.6
Issue Date: 05/12/2024

Certificate Number 12124
ISO 27001:2022

Z5042164

Access Group HQ
Armstrong Building Oakwood Drive
Loughborough
LE11 3QF, United Kingdom

Table of Contents

Introduction

Our customers expect strong information security controls and need to know that any data we process is securely protected, along with their reputation. Likewise, it is essential for Access to protect our own assets as a Controller and we recognised that the best way of achieving that was to adopt good information security practices, ensuring continuing compliance with the recognised international standard for Information Security, which is ISO27001:2022.

We support this with additional certifications and memberships related to the products and services we provide all of which are available on our Security Portal - https://access-support.force.com/Support/s/gdpr-hub (registration required)

Access has been certified by Alcumus ISOQAR to UKAS Standards for ISO27001 current standard since 2014. Copies of certification are available on request from your account manager, or via the Security Portal.

This document is designed to align with the ISO27001:2022 Standard.

Scope

- All Permanent Employees, Temporary Staff / Contractors / Suppliers and Third Parties working for and with Access or its affiliates.
- Our software, services, hosting, payroll bureau, payments financial services & screening
- All Information Assets
- Our Data Centre providers and supporting services are all ISO27001certified. We are not permitted to include them in the scope of our own certification but do obtain their certificates to confirm compliance.

Risk

Access has a Security Risk Management programme that is applied throughout the organisation and is managed by the Cyber GRC team (under the remit of the Chief Information Security Officer). It includes all assets for both Access and Customers, datacentre relationships, reputation, staff, suppliers, technology, buildings, processes, procedures, and services.

- It is managed through the Risk Register utilising ongoing risk assessments and reviews, acceptable risk process and associated controls with Board Reporting.
- There is in addition, a monthly Board "Security SteerCo" who review the current Risk Status across the organisation to drive improvement and maturity in our Security posture.

Note: We do not share our Risk Register

Policies & Documentation

Access does not have one single Information Security Policy; we include a general statement in that document and use it as the overarching requirement. It is underpinned by a list of additional policies can be found on the portal.

The policies are reviewed annually as a minimum or when legislation or changes in the business environment necessitates. These are reviewed by subject matter experts and approved by appropriate Management with the exceptions being the Information Security Policy which is signed off by the CEO and the Privacy & Retention Policies signed off by the Data Protection Officer.

All policies and other informative documents relating to Information Security are available to our Staff via SharePoint, and for clients via our Security Portal (registration required) – or they are available on demand via your Account Manager

All the following controls referenced policies and requirements are audited both internally and externally as part of our ISO27001:2022 certification.

Note: *Access does not share Audit reports as they may contain information related to our Staff and Security*

Leadership

Leadership is designed to ensure segregation of responsibilities and avoid conflict of interests – the key individuals for Access are listed below:

The Chief Executive Officer has overall responsibility for Security which is managed by the following: -

Chief Product and Engineering Officer – Who are responsible for Hosting, Information technology divisions, Internal IT/Service Delivery and provide support for reporting teams by ensuring that funding and resources are allocated.

Head of Security Operations – Hosting - Cyber security

Directors and Managers are responsible for ensuring that the Information Security and associated policies and controls are adhered to by all staff working for them. This includes reporting incidents and requesting general security guidance for new projects and initiatives within their teams.

Employees, Contractors, and others working on behalf of Access UK are responsible for complying with the information security policy and associated policies and controls.

The Data Protection Officer - Is responsible for

i. Defining and managing the privacy policy
ii. Oversight of training (managed by the Information Security Team)
iii. Ensuring compliance with relevant privacy legislation
iv. Provision of advice relating to legislation and best practice
v. Managing privacy related documents for distribution via our security portal
vi. Providing support and Guidance for privacy related incidents
vii. Engaging with all Access teams for new development – ensuring privacy by default and design.

The Information Security Manager and supporting team are responsible for

i. Planning internal / External audits
ii. Ensuring that the ISMS conforms to the requirements of ISO 27001:2022
iii. Reporting on the performance of the ISMS to top management
iv. Running risk programme
v. Determining policies and monitors compliance to those
vi. Works with the organisation to ensure compliance with Regulations pertaining to Information Security
vii. Manages training and compliance for staff.
viii. Phishing tests and awareness

Contact with Special Interest Groups and Authorities

Access maintains a comprehensive list of special interest groups and authorities relative to every area and software division of our organisation.

We subscribe to newsletters and forums, vendor groups and use these sources to obtain up to date information on legislation and of course threats and vulnerabilities.

Legal and Contractual Obligations

Access has identified and holds a list of applicable legislation and contractual requirements which further details how we comply as an organisation.

Access undertakes quarterly Management Reviews at both the operational level and additional Board / "SteerCo" level reviews to determine strategy, budget, and risks.

Human Resource Security

Recruitment & Screening

Access ensures that all recruited staff and Contactors have appropriate skills and experience for the role and a job description that needs to be verified as follows: -

The following screening checks to BS7984 standard are undertaken for new employees / contractors who will have access to customer information.

- Standard DBS
- Right to work
- Employment history
- Education
- Qualifications
- References
- Credit checks for financial staff
- Enhanced DBS checks for staff working in the Education Sector

Note: We do not repeat these checks during employment

Ongoing training and mentoring are in place to provide additional support and skills and mandated through Employee Success Plans.

Contracts and Terms of Employment

Contracts are signed by all employees and contractors, and those contractual agreements include Confidentiality / Non-Disclosure / Requirements to comply with all Information Security policies and associated requirements.

The contract specifically refers to the Access disciplinary policy that may be invoked in the event of a breach or non-conformance (depending on severity, intention, and other circumstances) and could result in termination of employment. These requirements are applied up to two years following termination of Employment depending on role.

Security Training & Awareness

All staff – within their first week, must read and confirm their acceptance to various policies within our Learning Management System – a summary of which is sent to the Information Security team weekly.

Staff must also undertake an online training course – comprising of 5 Modules (with an emphasis on Data/ Cyber) followed by a test that requires a pass mark of 85%. There is additional training for Managers and various technical roles and training is repeated annually.

Our training programme is supported by further information included in Staff Inductions and additional awareness campaigns / phishing tests etc. throughout the year.

Leavers and Movers

Our Joiners, Leavers and Transferees process is managed through automatic notifications from our HR Software as follows: -

- Most systems have Single Sign on applied and AD accounts are set to expire on leaving date.
- Email notifications are sent to a designated group of individuals following any change / creation of the Employee Record and a "FreshService" ticket created.
- The FreshService ticket includes an 18-point checklist that must be completed for leavers and movers, this covers retrieval of assets, removal of access rights, termination of card access for offices, removal from systems, changes of password etc.
- If an employee moves team, existing access is removed, and a new profile applied.
- Entry Badges are disabled on termination date.
- It is the Manager's responsibility to ensure that all assets are retrieved from a summary provided by the Service Delivery Team
- Leavers are removed from the "Active Directory" to prevent any access to our network, email, and other apps, where installed on personal devices.

Assets

All assets are documented and have assigned owners who are responsible for both determining risk and maintaining an inventory.

All technology Assets are recorded and maintained within Fresh Service

Asset	Owner	Custodian/s
Financial	Chief Finance Officer	Financial Controller & Head of Legal for Trademark & IP
Sales & Marketing	Chief Sales Officer / Chief Marketing Officer	Marketing and Sales Teams
HR Records	Chief Employee Success Officer	Head of Employee Success
Building & Contents	Chief Employee Success Officer	Facilities Manager/ Staff
Hosting Technology	Chief Product and Engineering Officer	Divisional Director of Operations
Internal Technology	IT Director	Head of Service delivery / Information Security Manager
Access Software & Code	Chief Product and Engineering Officer	Director of Development and Head of Development "Security First" Heads of Product & Divisional Leaders
Internet Domain names & Web sites	Chief Marketing Officer	Marketing team
Customer Data	Head of Legal Data Protection officer	All Access staff who have access to it
Clients	Chief Sales Officer / Chief Customer Success Officer	Account Managers and supporting teams

Information Classification

Access ensures protection of all information and records in its custody. The handling, labelling, storage, transmission, and disposal of Assets and all Media is covered in the Information Classification and Handling Policy according to a Classification Matrix.

Access uses the following levels of classification.

- Confidential (secret) – All data and information belonging to customers no matter what the category or type.
- Restricted - Limited to Access, Customers, and potential customers
- Internal - Access staff only
- Public

A combination of the above may be used i.e., Internal Restricted

Hard Copy media

We no longer store hard copy documents. They are scanned into our document system and destroyed using cross shredding.

We also no longer use tape backups, transport backups off site or move data by physical means.

Acceptable use of Assets

The Acceptable Use policy is a summary of controls that pulls together many of the key requirements included in other policies but which we feel are mandatory to avoid staff having to read every policy item that may or may not affect them. We do mandate sign off those policies or associated quick guides where indicated (in blue) and all topics listed are covered in our training programme.

The policy covers: -

- Classification
- Data Privacy (this is also the biggest module within our training programme)
- File sharing and Cloud storage
- Computing Equipment
- Remote working requirements
- Mobile device use
- Portable Media
- Supplied Media
- Password security
- Access Control

- Network and Cyber
- Incident reporting
- BCP
- Physical Security
- Clear Desk / Screen (auto lock 10 minutes)
- Providing remote support
- Leavers and what is expected.
- Staff acceptance

End of life Assets

Desktop Computers / laptops are securely "wiped" using proprietary software / de-gaussing and once validated completely clean, are often offered to charities but if beyond use are collected by specialist organisations under the Weee directive.

Servers have disks destroyed by vendors or specialist agencies who provide certificates of destruction, or we destroy the disks ourselves.

Access Control

Access to systems, networks and data is managed through pre-determined Role based Access Control, provided on a "least privilege" basis with segregation of duties applied as detailed above. Any requests over and above what is automatically provided, such as elevated rights must be requested via "Fresh Service", can only be permitted with business justification, and requires Director Level, Asset owner and Information Security sign off.

All accounts are unique and identifiable – sharing logins is a breach of policy and liable to disciplinary action.

Logins for customer systems in the Access Hosted environment are held in Delinea secret server.

There is no access to customer systems except from our own network. This must be from an In Tune Portal (MDM) registered device, using Global Protect VPN with MFA

All access to client systems and critical assets is audited and verified between 30 – 180 days depending on the classification of the contents.

Access to source code is restricted as follows:

- **Access Software** – The relevant development team only (GitHub)
- **Operational Software** – The Internal Service Delivery team only (restricted share)

Users are responsible for safeguarding login and password information and are not permitted to share or disclose either. Password management controls are documented within both the Access Control and Secure development polices.

Password policy depends on the age/ type / classification of the associated system by typically as follows.

New and acquired systems must be configured to ensure best practice password management.as recommended by NIST or minimally as follows. Systems that are not able to have these controls applied are reviewed for options and where possible – Access Identity is applied to mitigate risk.

Password complexity and requirements may vary from system to system but where possible passwords requirements should be designed as per Active Directory

- Min Length of Password = 14 chars / Max 256
- Min Complexity = a special character and Capital needed
- Expiry = Complex passwords – No expiry
- History = Last 10 passwords not allowed to be reused

Other systems - passwords must be 8 or more characters long and contain characters from 3 or more of the following groups:

- Uppercase
- Lowercase

- Numbers
- Symbols
- The new password must not be the same as a password used the previous 10 times.

Password expiry should be no longer than 90 days – except where pass phrases are used. These should be between 20 and 256 characters, set not to expire more than annually on recommendation from Security specialists/NIST.

We do not permit third parties to access our network unless required to support one of our own systems and only where In-tune or other VPN Controls have been applied.

We do not permit access to client data by Temporary staff or Contractors.

Cryptography

Cryptographic keys for both our software and Hosting environment are maintained by our technical teams and restricted to divisional heads or designate. All keys are typically managed by Access except where we have procured third party hosting services.

Access systems and software are encrypted for data in transit and at rest (this information is documented within the product fact sheets available on our Security Portal)

Encryption used offers at least 128-bit security with AES-256-bit technology wherever practicable.

Most Access hosted data is encrypted at rest both within the production and backup environments.

Physical & Environmental Security

Secure Areas

Assessments have been performed all our buildings and offices to identify any security risks both for access and BCP purposes.

The physical security assessment also determines whether environmental risks need to be considered and managed, such as flooding, loss of power, road and rail access, inclement weather and so on to ensure that mitigating controls are applied,

Staff access is generally by Salto Card (or Landlord issued) badges on a lanyard. The badge designates what areas of the building and what Access offices can be accessed freely, where offices have comms/server/ secure areas, these are covered by CCTV and accessible only to those staff that require access for legitimate business purposes.

Staff are required to wear their Photo ID badges (visibly) and where staff do not have their badge, they are provided a temporary one with a blue lanyard that is timed to expire at office closure. These are checked in and out by a designated individual.

Visitors provided temporary badges with lanyards that clearly identify them as such, they are required to sign in and out of each office and are not permitted to walk around premises unaccompanied and are not permitted to access any secure areas.

Typically Access no longer processes customer data within our offices and all access is remote unless data needs to be collected for Support / Development purposes (see Collection of Data for Support Purposes)

Information relating to Data Centres is provided as follows: -

Access Managed Hosting – Hosting Security Overview (available on our Portal or on request)

Non-Access Managed hosting/ Cloud – within the product fact sheets where we provide links to the providers web site. Some may be included within the fact sheet document itself.

Equipment

Within the offices, computing equipment is position. to ensure the least risk both in terms of internal services (sprinklers etc) and out of view of windows and common walkways.

Information related to the Data Centres can be found on the Hosting Security Overview document on our Security Portal or through associated links on the product facts sheets where not hosted directly by Access.

All supporting utilities are protected where necessary and there are maintenance agreements and testing regimes in place for those.

There are processing in place for removing assets and how they must be managed outside the environment.

There are Clear Desk and Clear screen requirements that are documented within the Acceptable Use Policy

Operations Security

All teams have operational procedures to ensure that security and quality is maintained thought both BAU and Project/ Development lifecycles. These are available through various means depending on the team but must be internal systems such as One Drive, the Network, Internal SharePoint, or Internal Wiki for example.

Change Management

Software development is managed through Agile Methodology with all changes logged and approved by the appropriate individuals (following scrum meetings) in JIRA.

Hosting /System change for Access Managed Hosting is recorded in Fresh Service and reviewed by a weekly CAB.

All changes are subject to privacy impact assessments, peer review, regression testing, and not released otherwise without CAB/ Senior Management sign off.

Capacity Management

Is achieved through a combination of technologies and monitoring with automatic alerts creating P1 tickets directly in Fresh Service.

Segregation of Environments

Development and Production systems are both logically and physically segregated in most cases.

Segregation of client environments within multi-tenanted databases is documented in the product fact sheets.

Controls against Malware

Access uses Cortex protection and Malware Bytes for Laptops and Desktops; Servers are protected by Carbon Black, Cortex and Microsoft Forefront within the Access managed hosting environment. Other AV protection is documented in the product fact sheets. It is not possible for any staff to disable these services.

- Updates are issued and applied immediately on release.
- Scans are scheduled weekly as a minimum.
- Paolo Alto Firewalls are also in place.
- Microsoft 354 technology is used to quarantine suspicious mails.

Information relating to the Hosting environment can be found within the Hosting Security Overview document available on the Security portal and on the Product, Fact sheets where software is not hosted within our own dedicated environment.

Backups

All internal and hosted systems are backed up automatically according to a schedule and encrypted both during the backup process and at rest. More information on this is provided within the Product Fact Sheet

Logging and Monitoring

Access uses Rapid 7 SIEM to manage both our internal and CE hosted environment. All logs are stored as read only and retained for 1 year.

Each product fact sheet provides further information on audit functionalities and further monitoring by product.

All clocks are synchronised with the time zone of the jurisdiction.

Technical Vulnerability Management

Access uses multiple sources to manage technical vulnerability management.

- Notifications from Vendors
- Membership of appropriate forums, security and working groups
- Alerts from organisations Access subscribes to
- Staff notifications
- Vulnerability scanning (weekly)
- AV and Security Patch releases
- Automatic releases for protection through the Palo Alto Firewall feed from the Vendor

Information systems are regularly reviewed for compliance with the information security policies and standards. This includes but is not limited to.

- Penetration testing
- Weekly Vulnerability scanning
- Reviewing Security Management system reports and audit information

Please note that Access is not able to share Pen Test or vulnerability reports as they contain information related to our own security, we may provide management reviews on request. We do not permit clients to pen test our environment.

Software Control

Access typically locks down admin rights on user equipment unless specifically required for the role. Cortex is installed and provides alerts on any software being downloaded or installed.

Network (Including Cyber) & Communications Security

Networks are managed and controlled to protect information in systems and applications, using security mechanisms as follows:

- Manage Server Access.
- Minimising the External Footprint.
- Patching Vulnerabilities (ensuring they are tested and evaluated before they are installed to ensure they are effective and do not result in adverse effects according to criticality
- Minimising Attack Surface.
- Restrict Admin Access.
- Minimising User Access Permissions.
- Establishing Communications.
- Preventing the Use of programmes to overwrite system controls.
- Segregation of networks, production, and development environments
- Logging, storing, and reviewing access.
- Ensuring that all systems on the network are authenticated and all connecting assets are managed with In Tune compliance.
- Utilising multiple security solutions such as
- Layer 7 Firewalls
- IDS/IPS/Malware/Threat protection
- Behavioural Analytics & Heuristics endpoint protection
- Phishing Protection
- Network Segregation
- MFA
- Conditional Access Controls
- Deployment of segregation of networks
- Implementing formal transfer policies, procedures, and controls (encryption) to protect the transfer of information both for data and email.

Monitoring

Access uses a Rapid 7 SIEM to collate all event and operational logs and this is monitored 24x7x365 We have business logic alerts built into the technology that can identify large packets of data moving around the network. The Palo Alto firewalls also monitor all network access to and from the internet. Fact sheets detail other monitoring capabilities for non CE Hosted Products.

Detail on how Access complies with the NCSC Principles – can be found on our Security Portal

System acquisition, Development & maintenance – Secure Development

Delivering secure and reliable software can only be achieved through sound security policies, process, and best practice. The Security First programme is one of the highest priorities in Product Development, and it is governed under the leadership and responsibility of the Chief Technology Officer; Managing Director CE; Director, Portfolio Management, and the Security Steering Group. Each role provides valuable input that ensures the overall success of the program. Here is an overview of their respective responsibilities:

General

Any new system or changes to existing systems are subject to auditable documentation, testing and acceptance with management sign off and consideration given to all legislative and security policy requirements. DPIA's are provided for all new development projects and significant changes to existing infrastructure.

Test and live systems are segregated in all cases and test data used is anonymised or "dummy" data unless a client has specifically provided a copy of their data during the UAT phase of an implementation.

Software Development

Secure design is a culture and methodology that constantly evaluates threats and ensures that code is robustly designed and tested to prevent known attack methods. Threat modelling is integrated into release planning.

Threat Modelling
Pro-actively prepares for potential threats, instead of reacting afterwards. Documents the whole application and gives Development teams a better understanding of the application and an insight into potential security issues. Enables us to identify and address the greatest risks.

Static Analysis using SonarQube
SonarQube provides automated code analysis that inspects source code without executing it. Security and code quality issues can be identified as part of the continuous integration (CI) to enforce quality gates that prevent vulnerabilities from being released.

Software Composition Analysis with WhiteSource & AppCheck
WhiteSource provides automated code analysis that identifies the security and license risks of our open-source usage. It enables us to identify all of our Free and Open-Source Software (FOSS), helps us ensure that we are correctly using permissive licenses and that all of the libraries are up to date and do not contain any known vulnerabilities.

Penetration Testing
Our external partners perform Penetration Tests to simulate targeted attacks on our software. These tests are completed as part of the acquisition process and at regular intervals for our products.

Considerations within product development cycle
Injection Flaw (specifically SQL)
Security Vulnerabilities
Secure Communications
XSS Vulnerabilities
Session management
Malicious Code
Authentication
Pen testing for Major Releases

Our Product Fact sheets are the software DPIA documents - these are published on our Client Security Portal along with other supporting information.

Developer Training

All Product Development staff complete mandatory Security First Essentials training to make them aware of the key elements of the programme and the role they play within it.

Our Developers and technical staff will additionally complete annual mandatory training focussing on secure coding and OWASP top ten vulnerabilities.

High quality training is freely available that covers a wide range of security topics, such as common vulnerability types and how to avoid them, general security guidance and principles, use of cryptography, etc.

Attendance and completion of all training is monitored through our Learning Management System in order to ensure that all employees comply with expectations and requirements.

System Development

Security starts at design stage and includes additional controls such as "hardening" in line with NIST and CIS standards then pen tested. Access uses scripts and technology to ensure consistency with system builds.

All system development and changes are managed through the weekly CAB.

Supplier Management

All new suppliers are subject to a review process before being added to the Supplier list. This review includes: -

- Service Provided
- Associated risks
- Legislative requirements i.e Privacy
- Security Controls (where applicable)
- Security Arrangements
- Certification
- Terms and Conditions reviewed by Legal & Procurement for contracts with TCV (Total Contract Value) of £100k+
- Tier Categorisation
- Certification validation
- Supplier security assessment document
- Use of risk assessment platform for onboarding and ongoing monitoring dependent on risk tier.

If the supplier does not meet the criteria for approval by our Information Security Team, the supplier application will be rejected. This may be followed by an review on request in which case mitigating controls may be applied, the supplier approved and monitored.

Non-Disclosure and appropriate Data Processing agreements are required for any service that has a bearing on Information Security or personal data and we require controls and security no less than our own for a supplier to become approved.

We do not permit third party access to our Network or systems, unless providing technical support to Access specifically

Tier 1 (critical suppliers or those that are providing services where personal data is concerned) are reviewed annually to ensure that the contracts and any associated controls are adequate and compliant.

Any significant proposed changes to services are submitted to information security for supplier review before approval.

We reserve the right to audit suppliers at any time as outlined in our Supplier Code of Conduct.

The Fact Sheets provide a schedule of sub-processing in place for each product.

Incident Management

Access considers incident management as any event that affects the Confidentiality, Integrity, or Availability of Assets. This may be insignificant or major, but all are all referred to as incidents.

Staff are encouraged to report incidents no matter how trivial they may seem (even suspected), and these are logged in FreshService for audit and tracking purposes. An incident report is mandatory for any data breaches and corrective & mitigating actions are taken in all cases, lessons learned are documented and where relevant the Incident report is shared with the client.

If necessary. issues may be included on the Risk Register for further consideration or processes modified. Additional training is mandated for individuals or Employees where human error is determined as a root cause.

Where an incident involves or has a direct impact on a client – that client will be contacted as soon as the incident is identified "without undue delay" to ensure that any subsequent reporting by the controller can be fulfilled. The method of communication will depend upon the nature and severity of the incident (see section on breaches)

Access provides the affected party with the abovementioned incident report which contains information relating to the incident, the timeline, actions taken, summary, any remediation required and follow up tasks if relevant.

We additionally use technologies including but not limited to Pager Duty, MS Office tools and Prisma Discovery for incident management and investigation, but Access has an agreement with an external, professional computer forensic organisation for incident response and forensic services if required.

Data Breaches

We consider data breaches within the remit of Incident Management as described above and do not have a separate process.

Out contractual obligation is that breaches must be notified "without undue delay" in order that the controller may notify the supervising authority if necessary.

Please Note: Access does not increase liability within contracts because of the amendment within the GDPR that makes Processors equally liable for breaches they have caused. We do however have Cyber Insurance details of which are available on the Security Portal.

Business Continuity

Access considers Business Continuity in the same context as Disaster Recovery, and both come under Incident Management as the situation would be the result of an incident. It is the ensuing recovery that determines whether it is a short-term disruption or long-term problem. Our BCP documents provide for both and are available on our Security Portal or on request, but we do not share our plans as they contain information related to security and staff.

Possible scenarios covered: -

- DDOS
- Cyber Attacks
- Hacking / Ransomware
- Data Exfiltration
- Office unavailability (outages and access) / Building Loss (and partial loss)
- Staff / Pandemic
- Terrorism / Bomb threat
- Environmental threats
- Airport / Flight
- Loss of facilities
- Loss of supporting infrastructure / Transport
- Weather
- Systems
- Key suppliers

Our hosting division undertakes weekly back-up and restore testing with desk top walk-through's every 6 months using an isolated comprehensive restore test to minimise disruption.

Our office plans are rotationally tested.

Note: We do not incorporate customer testing or requirements due to the scalability of numbers and we do not share any operational documents such as BCP testing exercises as they contain sensitive internal information on systems and staff.

Compliance

See Legal and Contractual Obligations

Access ensures that it is licenced for all products and services it procures and uses.

Privacy and Protection of Personal Data

Governance

Access is registered with the Information Commissioners office (Z5042164) and handles all data in accordance with the UK GDPR, the General Data Protection Regulation and other privacy requirements in other countries we operate in.

Data Processing Agreements

Unfortunately – Access cannot sign individual client DPA's.

We provide Product Fact Sheets, based on DPIA requirements for GDPR legislation and this support the Details of Processing for data sharing agreements as referred to in our Terms and Conditions as follows:

(www.theaccessgroup.com/standardtandcs).

Schedule 2 - Data Processor Terms

Section 1 - Definitions - Included in Terms & Conditions

Section 2 -Processor Clauses - Included Terms & Conditions

Section 3 - Details of Processing - Product Fact Sheets

Section 4 – Security Standards (Technical and Organisational controls referred to in the Ts and Cs as Our Security Standards, fact sheet and other supporting documents which are available on the security portal)

Why does Access Manage DPA's in this way?

The reason Access manages DPA's in this way is that apart from the Obligations and Rights, processing information will inevitably change over time as products are enhanced, further products or modules taken, legislation amendments etc. When a DPA is signed, the information is static so those changes or others not detailed makes a DPA an indefinite moving target which would need to be updated frequently ensure it is adequate for purpose.

The impact of multiple and frequent changes would also have a financial impact as it would necessitate a large team, the cost of which would need to be reflected in the pricing structure.

Therefore, in order to maintain validity and accuracy in the most efficient and cost-effective way, we provide product fact sheets and associated documentation (which are updated constantly) to support the DPAs. They are available on request via the Account Manager or directly from the security portal.

Storage/Processing – Geographical Locations

Information related to storage / processing and support is detailed on each product fact sheet.

Access maintains a Data Register of all hosted information.

Collection of data for support / product implementation purposes

Technical Support often need access to client systems to resolve issues but on occasions they may require a copy of the data to replicate an issue. The data can only be collected with explicit agreement from the client using the controls listed below.

- Any device that is being used to process client data, must be registered on the In Tune Portal and connected to the Access network via Global Protect.
- No data can be collected without explicit, written permission from a customer – whether for support or project purposes
- Hosted data cannot be collected directly by support, a request is made through the Data register form to the hosting team. (In order to maintain an audit trail and ensure segregation of duties)
- Data must be transferred via Access Collaborate, sftp or other secure means designated by the customer and immediately recorded on the data register Information including the purpose for collecting, together with the client approval.
- The collected data must be deleted from the transfer mechanism immediately on transfer to secure storage.
- The Secure storage must be an Access issued Encrypted hard drive (where provided) a Bitlocker enabled PC/Laptop (XTS-AES 256-bit hardware encryption / FIPS PUB 197) or specific designated network area – restricted by logical access control.
- If the data is shared with any other member of Access (development for instance) a second data register entry must be created.
- If it is likely to be required for over 90 days – written consent is required from the client and the consent uploaded to the record.
- Once the data is no longer required – It must be deleted everywhere and from Recycle bins/deleted items areas. The data register record/s can then be closed.
- Email alerts are sent to Managers and Information Security if the data exceeds the agreed retention. Data retention is considered a breach of the GDPR regulation, and these alerts reflect that position. Repetitive failure to adhere to the above requirements can result in the disciplinary process being invoked.

Retention

Access does not impose retention policies on client data other than as detailed in the Product fact sheet for Backup purposes and on termination of contract.

Exit Policy

Access only processes data for the duration of a client contract. Once notice is given, a customer will be provided with a form to complete indicating their wishes in relation to return or deletion of data. The process is managed through the data register and after deletion, the customer is informed, and the register entry closed.

Access offers: -

- Deletion
- Return of data in storage format – IP removed.
- Other – may incur chargeable services.

Deletion of data is completed no later than 30 days from Termination of Contract.

Security Review

As well as our internal audit programme, offices are subject to external audit by Alcumus ISOQAR to UKAS requirements on a rotational basis. The Access Group is Cyber Essentials Certified. Access has 100% compliance on the NHS Information & Data Protection Portal.

Appendix 1 – Portal Guide

Our portal is here: https://access-support.force.com/Support/s/gdpr-hub

If you haven't registered, select "not a member", complete the form and as soon as our community team have validated you as a client – you will be informed that your account is active.

SUBJECT	WHERE TO FIND IT
Access control within products	Product Fact Sheets
Annex 1 of our Terms and Conditions	Product Fact Sheets
Business Continuity – General	Organisation and Certificates
Business Continuity	Hosting
Categories of Data Subject	Product Fact Sheets
Categories / Special categories of PII processed	Product Fact Sheets
Certificates /Accreditations	Organisation and Certificates
Company Information	Organisation and Certificates
Contract GDPR Addendum for non-standard T's & C's	Our website
Data Centre / Hosting Security Information	Hosting & Product Fact Sheets
Data Flows – Hosting Environment	Hosting
Data Flows – Product	Product Fact Sheets
Details of Processing (Annex 1 of Ts & Cs')	Product Fact Sheets
Data Processing Agreements	Included within our Standard Terms and Conditions
Duration of Processing	Product Fact Sheets
Encryption	Product Fact Sheets

SUBJECT	WHERE TO FIND IT
Fulfilment of Rights within our software	Product Fact Sheets
GDPR / Privacy Specific Request forms and processes	Privacy / GDPR
General information relating to ISO27001	Organisation and Certificates
ICO Registration Information	Privacy & Information
Insurance	Organisation and Certificates
Nature of Processing	Product Fact Sheets
Organisation Security Overviews & QA	Organisation and Certificates
Our Compliance Summary	Privacy & Information
Policies	Policies
Purpose of Processing	Product Fact Sheets
Retention information by Product	Product Fact Sheets
Retention Schedule	Privacy & Information
Risk	Organisation and Certificates
Security of Product	Product Fact Sheets
Staff Training	Organisation and Certificates
Statement of Applicability	Organisation and Certificates
Storage of Data / Location / Backup	Product Fact Sheets
GDPR Subject Matter	Product Fact Sheets