20/12/2022

# Access PeoplePlanner

## FACT SHEET

# Contents

## Introduction

This Product Fact sheet provides the detail required for Data Privacy Impact Assessments, processing information that supports our terms and conditions and general security relating to the product and associated services.

Further information related to security can be found on our Customer Security Portal (Registration required)

This product is available in the following regions: UK

## Subject Matter

- Privacy Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
- It protects the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

## The Product

| | |
|---|---|
| Name of Product / System | Access PeoplePlanner |
| Set up options | Saas |
| Purpose of the Software | Operational Platform for Community & Residential Care Providers. Functionality includes Applicant, Employee, CRM, Customer, Service User Management, Scheduling, Monitoring, Reconciliation, Payroll and Invoice production and management |
| Product Category | Health & Social Care |

## The Data

| | |
|---|---|
| Duration of Processing | Processing will continue for the duration of the active contract. Access does not apply retention schedules to client data other than for backups (see backup section) and deletion of data on termination of contract in line with our Exit policy (unless there is a legal requirement for Access to retain the data) |
| Nature of Processing | Hosted/ SaaS - We receive data uploaded to the service by users, which is stored in a cloud environment in accordance with the options selected by You. Users may instruct the service to share some or all of the data with other users or groups/classes of users. |
| Purpose of Processing | The data is entered or imported into Access Care Planner via PeoplePlanner, or by the client<br>The type of data captured, held, and processed is configured by our clients / based on their needs |

| | |
|---|---|
| Categories of Data Subject | Data may be related to the following categories of data Subjects:-<br>Medical Patients Applicants Employees Customers Prospects Service Users Carers. |
| Personal information, that on its own or with any other data in the system, can identify an individual | First name<br>Surname<br>Address<br>Phone number<br>NI Number (Applicant/Employee).<br>Next of Kin<br>Emergency Contact Details (Name & Address)<br>Gender<br>Email Address<br>Other fields configurable by the client |
| Special categories of Data stored<br>o Race / Ethnic origin<br>o Political opinions /Religion / Philosophical beliefs<br>o Trade union membership<br>o Genetic data /Biometric data / Health<br>o Sexual Orientation / Concerning a natural person's sex life | Race<br>Ethnic Origin<br>Religion<br>As configured by clients<br>Processing permitted under GDPR due to the nature of the service |
| Legal reason for Access processing the data | Contractual |
| **The Rights of the Individual** | |
| Subject Access Requests | We will be supplying our clients through the latest version with the ability to fulfil both these Rights using an export to spreadsheet |
| Portability information | There are spreadsheet exports within People Planner that provide this data in a human readable and machine readable format. This can be exported by the customer |
| Data Amendments | Yes by the client with appropriate permissions can edit personal information via the UI. If the personal details are supplied via an internal integration (Such as Access People), These details can be amended in the integrated system, and not on People Planner. |
| Details of Automated decision making processes | Yes Access People Planner has planning rules like Maximum Hours Per Day, Maximum Hours Per Week, Training & Qualification Rules (e.g. can they deliver the required care to the client), White Lists/Black Lists, Clashing / Near Clashing.<br>Based on client configuration, we would expect the client to inform their users of the detail |
| Right to Erasure (Right to be Forgotten) | Functionality in the product will enable a user with the appropriate permissions, to obfuscate the data based on your retention requirements |
| Bulk data archiving/ deletion capability within this product | None<br>Due to issues with historical data and data integrity we do not provide any option, scripted or otherwise, to bulk delete or archive data |

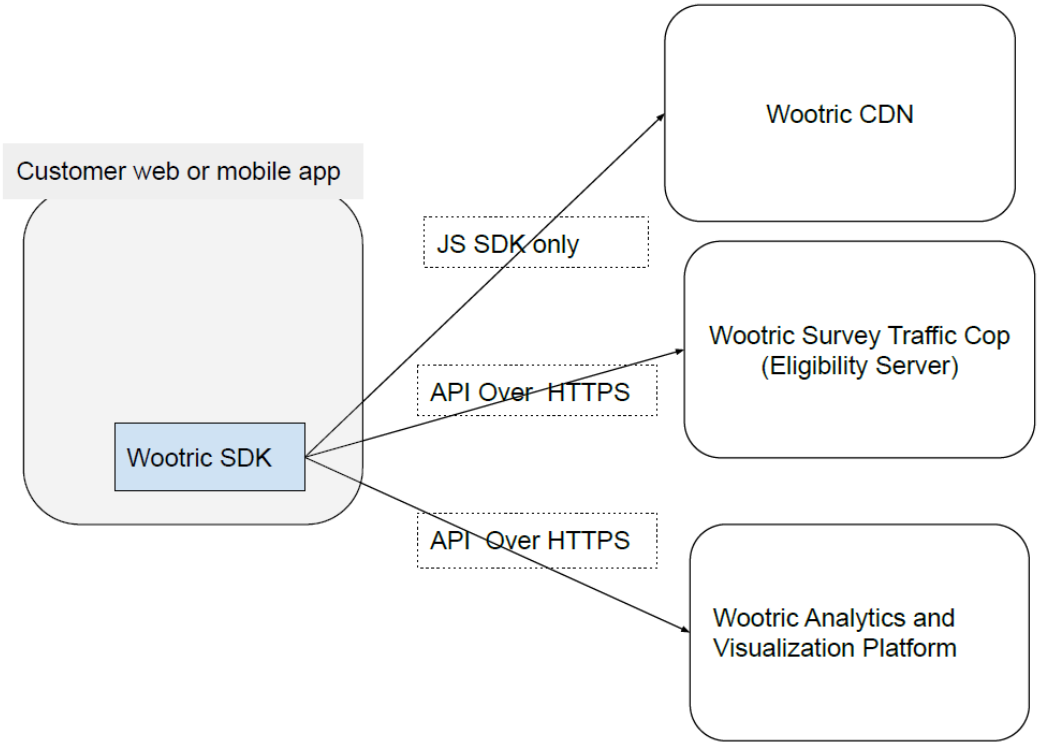
| | |
|---|---|
| Are clients able to set their own retention schedule | No |
| Anonymisation capability | Yes – Built in GDPR anonymisation tools. The tool is accessible via the UI by a User with the appropriate access permissions. CRM, Employee, Service Location and Customer records can be anonymised. |
| Pseudonymisation capability | No – Only full anonymisation supported |
| **Access Control & Auditing** | |
| Is this product available through workspace | Yes |
| Who - apart from the customer has ongoing access to client data? | Development, Support, On-boarding teams, Professional Services |
| Geographical Location of those teams | UK & Romania |
| How do technical support access the software when calls are logged? | Via the UI and Support User |
| Who has access to the database? | CHS DBAs, 3rd Line Support, Senior APP Developers |
| How do that team access the database for support and operational purposes | All access is via secure SQL jumpbox |
| Geographical Location of those teams | UK & Romania |
| How is access control to the product managed for customer users – what protocols does it support? | There are two methods of logging in to APP - These can be used individually or in combination - The first is direct access via inbuilt Username and Password authentication, the second is via single sign on via Access Identity (OAuth). No other methods supported. |
| Does the product support role-based profiles / who determines them and who administers | Yes, APP supports role based user access. This is managed by the Customers themselves. There is also an administrator access used by Support. |
| Password Policy | 6 with PP / 8 with Identity – user configurable |
| Password Security information | SQL Database - encrypted, using one way encryption |
| Password Expiry | APP does not support password expiry, however these options are available via Access Identity. |
| Number of log-in attempts before account is locked | Not supported for direct PP login/ Configurable with Access Identity |
| Successful and Failed login attempts recorded? | Yes, Login attempts are recorded, on both success and failure (TBC Access Standard) |
| Other areas of the software where actions are recorded and auditable | All Data Changes (outside of settings) |
| Storage of Audit Logs | Audit Logs stored in a database table, they are retained for a user definable length of time, the |

| | |
|---|---|
| | default configuration of which is 16 weeks, however automatic clear up can be disabled (i.e. stored indefinitely). |
| Is there an automatic time out after inactivity - please state what time | 60 Minutes |
| Does this product redirect to a Card payment provider | No |
| Third Parties that have access to the data | See Schedule 1 – Sub-processors |
| Outputs to other systems / externally or internally | Client Portal can be used to share data, but this in fully under client control |
| Is Wootric Feedback enabled for this Product? | Yes |
| **Product Security** | |
| Data Encryption in Transit | Yes- TLS and Secure File Transfer Protocol encryption |
| Keys Managed by | Access Cloud Hosting Services |
| Data Encryption at rest | Yes – Hardware based encryption managed by |
| Keys Managed by | Access Cloud Hosting Services |
| Email functionality | Yes |
| Email provider | Internally hosted SMTP server (smtp.com) or customer specified SMTP servers |
| Geographical routing of email | Canada (Data in transit applies) or Customer specified smtp servers |
| Data Storage formats | Main Storage is SQL Database for all data, Backups are in SQL Backup Format. Users can upload and generate documents which are stored in the database. |
| Cookie information | Session Cookies; Google Analytics. No personal identifiable information tracked. |
| **Physical & Network Security/Storage** | |
| Location of server / physical storage / file system/ Data Centre Provider / Geographical location | Telehouse London |
| Who manages the environment | Access Cloud Hosting Services |
| Firewall Information | Includes but not limited to Palo Alto and Cisco Firepower modules<br>Server Firewalls - Windows Firewall<br>Distributed Firewalls – VMWare NSX |
| Intrusion Detection | Access uses a combination of technologies<br>Layer 7 Firewalls<br>IDS/IPS/Malware/Threat protection<br>Behavioural Analytics & Heuristics endpoint |

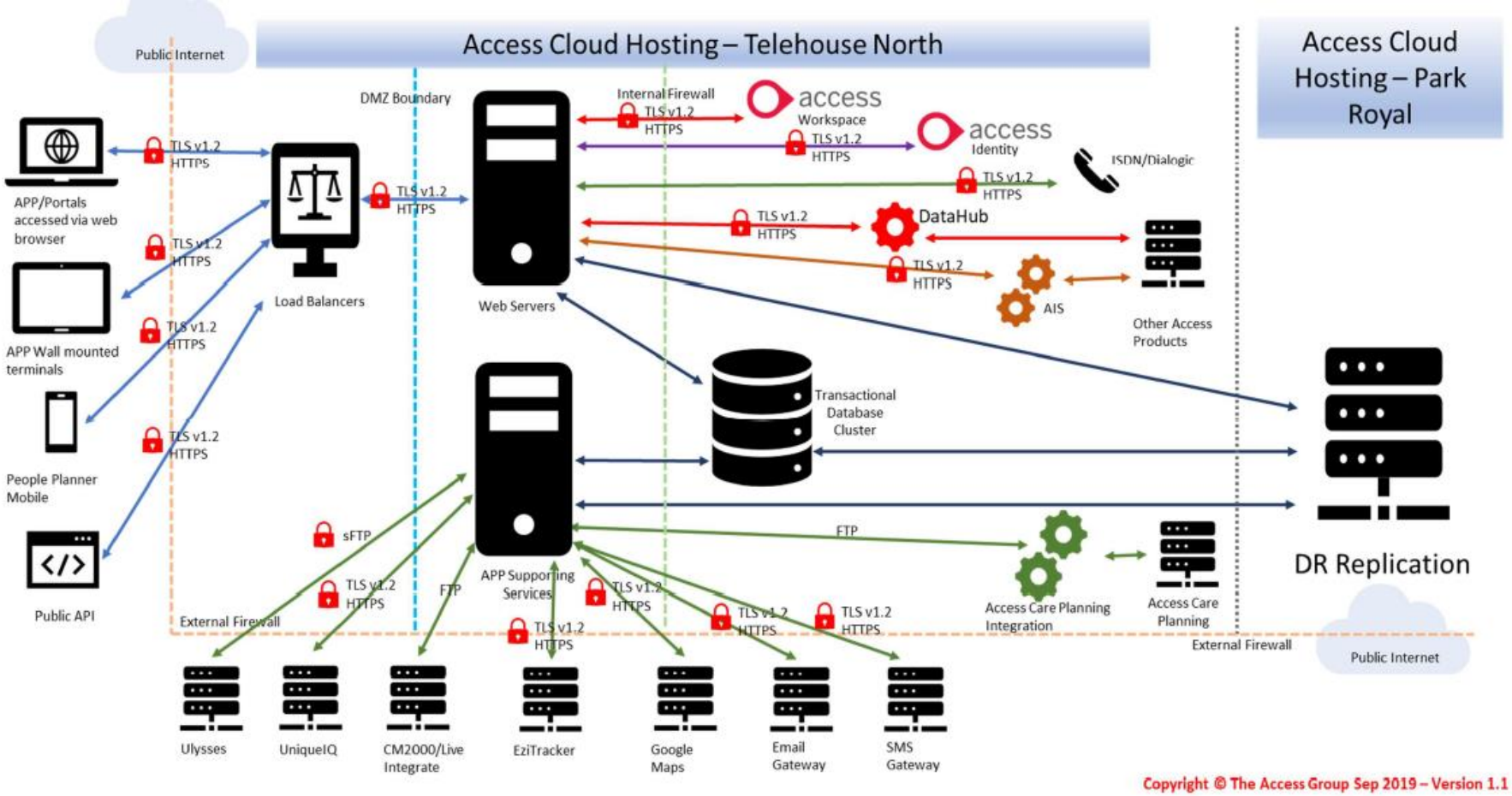
| | |
|---|---|
| | protection<br>Phishing Protection<br>Network Segregation<br>MFA<br>Conditional Access Controls |
| Antivirus in use on Servers | Cortex XDR |
| Other security features | Multiple – available in the Hosting Security Overview document on the Security Portal |
| Is this a multi-tenanted database? | No |
| How the client is data segregated from other Clients in the hosted / Cloud environment | Segregated at Database layer. Each customer has their own database. |
| Other set up options available (i.e. isolated/shared) | By default, instances share a website and have isolated databases on a shared database cluster. For larger customers, we can provide isolated website and database clusters. |
| Backup details / Storage and Encryption | Frequency<br>SQL Transaction log back up every 15 minutes 28 days<br>Daily (10 pm) backup 28 days<br>Weekly (Saturday) 3 Months<br>Monthly (1st of the Month) –<br><br>Retention<br>3 Months<br>Payroll 5 years<br>Backups are stored within a multi tenancy data vault and are encrypted at rest<br><br>Location:<br>Equinix LD3 - Park Royal |
| Backups managed by | Access Cloud Hosting Services |
| BCP arrangements | Details available in our BCP document on the Security Portal |
| Segregation of Production and Development environments. | Logically and physically |
| If there is a web service Is there a mechanism that restricts access to the Web Service | IP whitelist is supported in People Planner system |

| About the Mobile App | |
|---|---|
| Is there a mobile app | Yes |
| How is data secured between the App & the Server? | HTTPS (SSL) |
| Is Data stored on the device? (If yes, what data? for how long?) | Yes – Basic Service Duty information, visible for maximum of 999 hours past or future (user configurable) |
| Format of stored data | TBC |
| **Exit Arrangements** | |
| How is data returned to clients on termination<br>Access Provides / Self Service / Bit of Both? | Access provides |
| What is the standard format | .csv export of each database table |
| How is the data deleted or anonymised | Deleted |

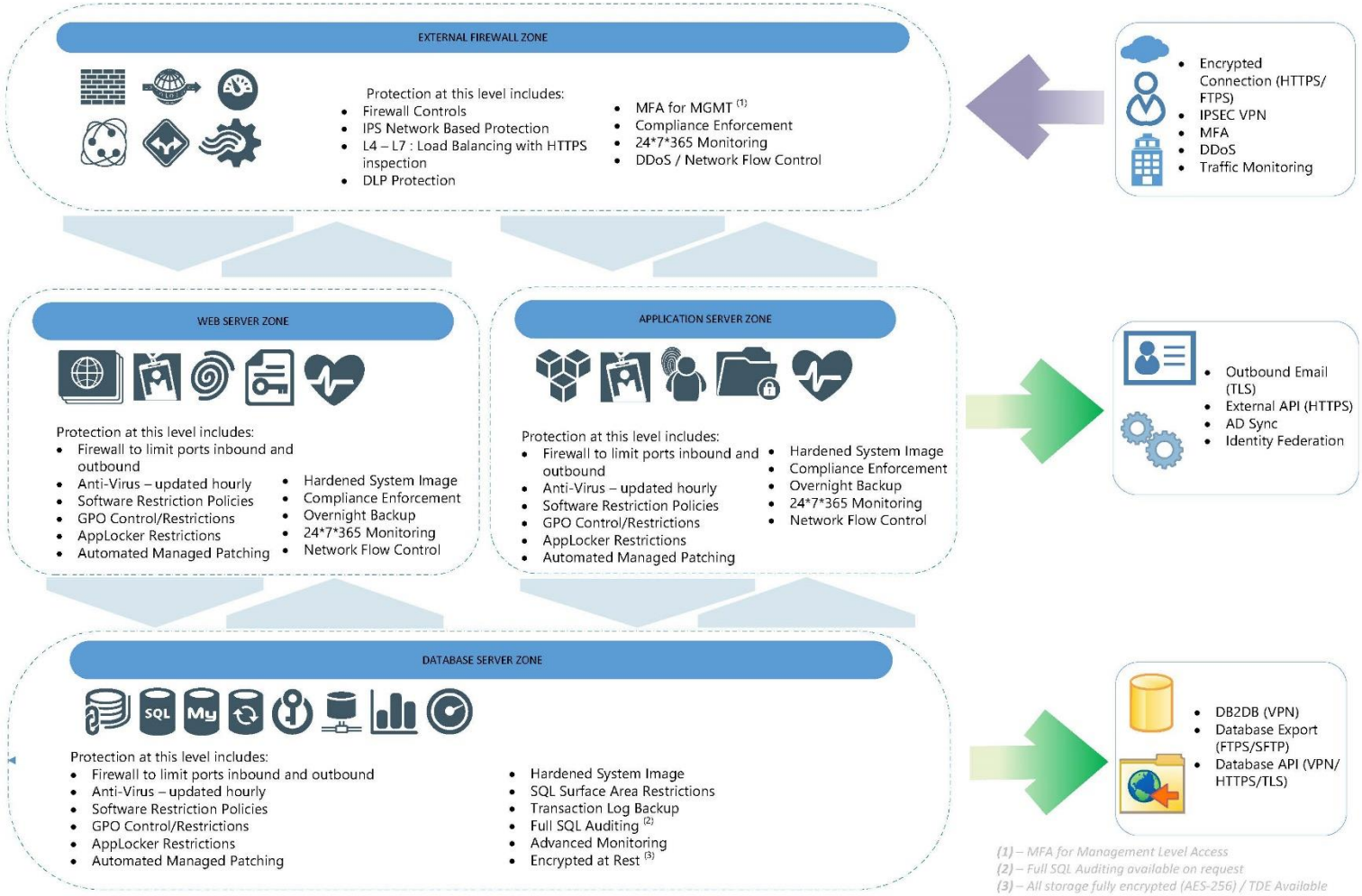
# Wootric Data Flow



# Product Data Flow



# Network Diagram




*(1) – MFA for Management Level Access*
*(2) – Full SQL Auditing available on request*
*(3) – All storage fully encrypted (AES-256) / TDE Available*

## Schedule 1 – Sub-Processors

| Sub-processor Name | Category | Sub-processor Main Location(s) | Nature of the Processing | Location of the Processing | Safeguards / Legal Data Privacy Frameworks |
|---|---|---|---|---|---|
| Access Workspace Australia Pty Ltd<br><br>(636482383)<br><br>Level 11, Tower B 821 Pacific Highway Chatswood 2067 | Affiliate | AUS | Hosting Infrastructure support for the AUS region<br><br>Out of hours infrastructure support for the UK/EU | UK & AUS | Intra-group data processing agreement |
| Access Workspace Romania (Co Reg: J35/2682/2007) | Affiliate | Romania | Support, Technical Support | Romania | Intra-group data processing agreement |
| In Moment (Wootric)<br><br>Corporate Headquarters 10355 South Jordan Gateway Suite 600 South Jordan, UT 84095 | Partner | USA | Wootric – provides product feedback from users by providing a survey and analytics platform for Access to collect, analyse, and act on feedback from end users (name & email only)<br><br>All communications from Wootric client-side SDK to Wootric server are over SSL through https protocol. Data is encrypted at rest.<br><br>https://www.wootric.com/developers/security/ | USA | Standard Contractual Clauses – storage only – Wootric do not have access to Data and this functionality can be disabled on request |

| | | | | | |
|---|---|---|---|---|---|
| Smtp.com | Business Partner | USA | Smtp mail functionality | Canada (data in transit only) | Standard Contractual Clauses. |
| Cloudflare | Business Partner | USA | We use Cloudflare as our WAF and Load-balancer, it is a globally based system to ensure redundancy, it will store IP addresses for the purpose of load balancing, but no other data is processed by it as the traffic is SSL encrypted. | Global | Contract inclusive of GDPR/data privacy provisions./ SCC's |
| Rapid7 | Business Partner | EU | SIEM Monitoring<br><br>Network data (including source and destination IP addresses and domains, approximate geolocation based on IP lookup, network traffic flows, communications metadata, machine names, and unique device identifiers)<br><br>User and endpoint behaviour (including user account activity & metadata, applications executed on endpoints, and accessed URLs)<br><br>Application logs (including firewall logs, DHCP/DNS logs, intrusion detection logs, malware logs, cloud service logs, proxy logs, file access logs)<br><br>Other relevant machine data which the data exporter elects to send to the data importer for processing.<br><br>Data is encrypted before it is pushed from the collector to the cloud. InsightIDR employs public key cryptography and challenge-response handshakes to ensure the security of data<br><br>User credentials are encrypted with bcrypt; credentials to connect with event sources are encrypted using RSA PKI (4096 bit keys). | EU | Contract inclusive of GDPR/data privacy provisions. |