Date: 8th March 2024

CallConfirmLive! and Finance Manager

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)

Subject Matter

- The General Data Protection 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.
- The Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

The Product

Name of Product / System	CallConfirmLive! and Finance Manager
Set up options	SaaS
Purpose of the Software	The collection of client/carer and scheduled visit data in order to deliver care based on contractual requirements.
Product Category	H&SC

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 : 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 collection of client/carer and scheduled visit data in order to deliver care based on contractual requirements.

Categories of Data Subject	For example Prospects, customers, business partners and vendors of Customer (who are natural persons) Employees or contact persons of Customer's prospects, Employees, Employees contacts, agents, advisors, freelancers, of Customer (who are natural persons) Customer's Users authorised by Customer to use the Services
Personal information, that on its own or with any other data in the system, can identify an individual	Name, Address, Postcode Mobile & Landline Number Email address Date of Birth NHS Number Social Service Number
Special categories of Data stored ○ Race / Ethnic origin ○ Political opinions /Religion / Philosophical beliefs ○ Trade union membership ○ Genetic data /Biometric data / Health ○ Sexual Orientation / Concerning a natural person's sex life	Health related data - Condition type - Medication data - Ethnic Origin - Religion
The Rights of the Individual	
Subject Access Requests	Customers can facilitate their own data SAR's through the system. Organisations using CMBI can extract the data. Organisations not using CMBI can use the Data Extract Wizard within CallConfirmLive! to manage this requirement.
Portability information	Data can be extracted by the tier 2 support staff upon request or via CMBI
Data Amendments	This is performed by the user organisation within the solution when an ammendment request has been recived from the Data Subject. Access can update records if required and authorised by the Data Controller, and this would be initiated through a Customer Support ticket
Details of Automated decision making processes	Carer scoring system used to determine the most suitable carer to be assigned to a care visit based on a point scoring system. This can be over-ridden by the user
Right to Erasure (Right to be Forgotten)	Users within the organisation can anonymise an individual's data in response to a Right to Erasure (Right to be Forgotten) request. This process removes all PID data from the record.
Bulk data archiving/ deletion capability within this product	Not inside the product but there is a business process that allows the business to bulk anonymise this data.

Anonymisation capability	The solution allows users with the correct permission to anonymise client record data
Pseudonymisation capability	No
Access Control & Auditing	
Is this product in Workspace / uses Identity	No
Who - apart from the customer has ongoing access to client data?	Support, Account Management , Centre of Excellence, Customer Success Team and Engineering Team but only when dealing with an incident escalation
Geographical Location of those teams	UK
How do technical support access the software when calls are logged?	Hosted solution controlled through Username and Password Unique credentials User must have a Citrix account and then a separate user account for the customer database they wish to access and must provide business justification (recorded)
Who has access to the database?	CE 2nd line Support Engineering Team CoE (as part of approved support work)
How do that team access the database for support and operational purposes	By default no access is given but access can be given on request as part of the approved support work via SQL Management Studio with Windows Authentication
How is access control to the product managed for customer users – what protocols does it support?	Username and Passwords The Microsoft Authenticator app is utlisied as the MFA solution Customer specific segregated databases
Does the product support role-based profiles / who determines them and who administers	Yes Pre-set and custom defined RBAC
Password Policy	Configuable per customer No minimum standard
Password Security information	Encrypted - custom
Password Expiry	Configurable per customer
Number of log-in attempts before account is locked	Configurable per customer

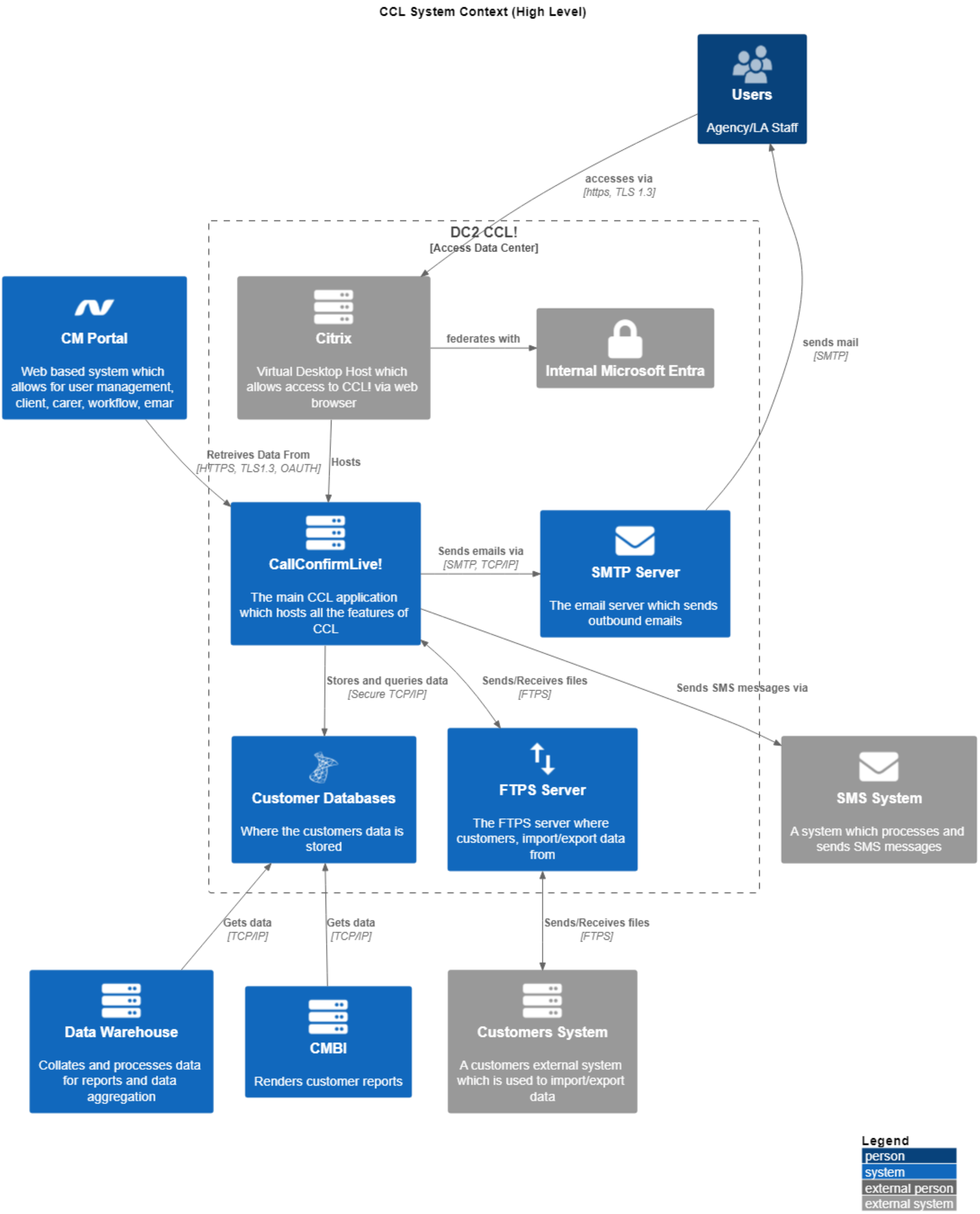
Successful and Failed login attempts recorded?	Yes, all login attempts and the related outcome are recorded in the User Logs and a report can be run to show this information
Other areas of the software where actions are recorded and auditable	The Auditing function has a set of basic fields that are audited, and customers can add in any others as required. There are some tables which haven't been coded to allow full auditing. *Note –running audit logs may affect the performance.*
Storage of Audit Logs	Where: Database tables and line logs Format: Plain text Storage time: Forever, 30 days on site & 8yrs in deep storage
Is there an automatic time out after inactivity - please state what time	120 minutes, however customers can change this.
Third Parties that have access to the data	PID can be surfaced through the data reporting software CMBI, if the customer has purchased this. PID is not made available to any other 3rd parties
Outputs to other systems / externally or internally	Data is not made available to any other system by default
Is Wootric Feedback enabled for this Product?	No
Product Security	
Data Encryption in Transit	TLS1.3
Keys Managed by	CE
Data Encryption at rest	256.AES
Keys Managed by	CE
Email functionality	Yes
Email provider	DC2 SMTP
Geographical routing of email	UK
Data Storage formats	SQL
Cookie information	None
Physical & Network Security/Storage	
Location of server / physical storage / file system/ Data Centre Provider / Geographical location	DC2 UK Based
Who manages the environment	CE

Firewall Information	We use a combination of products for Perimeter/ Server/ Distributed and Desktop firewalls including but not limited to Palo Alto, Carbon Black and Windows
Intrusion Detection	Cortex XDR
Antivirus in use on Servers	All Windows Operating Systems have resident supported Anti-Virus installed. This includes but is not limited to Carbon Black, Cortex and Palo Alto products AV software is controlled and managed via a centralised management portal in line with the following policies: • Compliance – alerts are generated by non-compliant devices e.g. devices that have not updated recently or have un-acknowledged alerts. • Definition Updating – manages the updates from a centralised location against local and supplier repositories • Schedule – all servers are set to run a scheduled AV scan of all files and settings nightly • Product Updates – manage the deployment of product updates and patches • Alerting – centralised alerting to our Network Operations Centre and Security Officer from managed clients • Tamper Protection – all resident AV has Tamper Protection deployed to prevent the disablement or alteration of local policies without authorisation from the central management portal • Behavioural Monitoring – next gen AV products monitors application behaviour against known “good state” behaviour is automatically blocked and any alerts are generated to our Security Administration team for investigation and remediation
Other security features	N/A
Is this a multi-tenanted database?	Yes
How the client is data segregated from other Clients in the hosted / Cloud environment	Data is segregated within Databases per organisation which is then further segregated using a provider and contract filter/permission. Users can only be assigned a subset of their organisations data access, if data access for their organisation is revoked then this change is also propagated to all of its users.

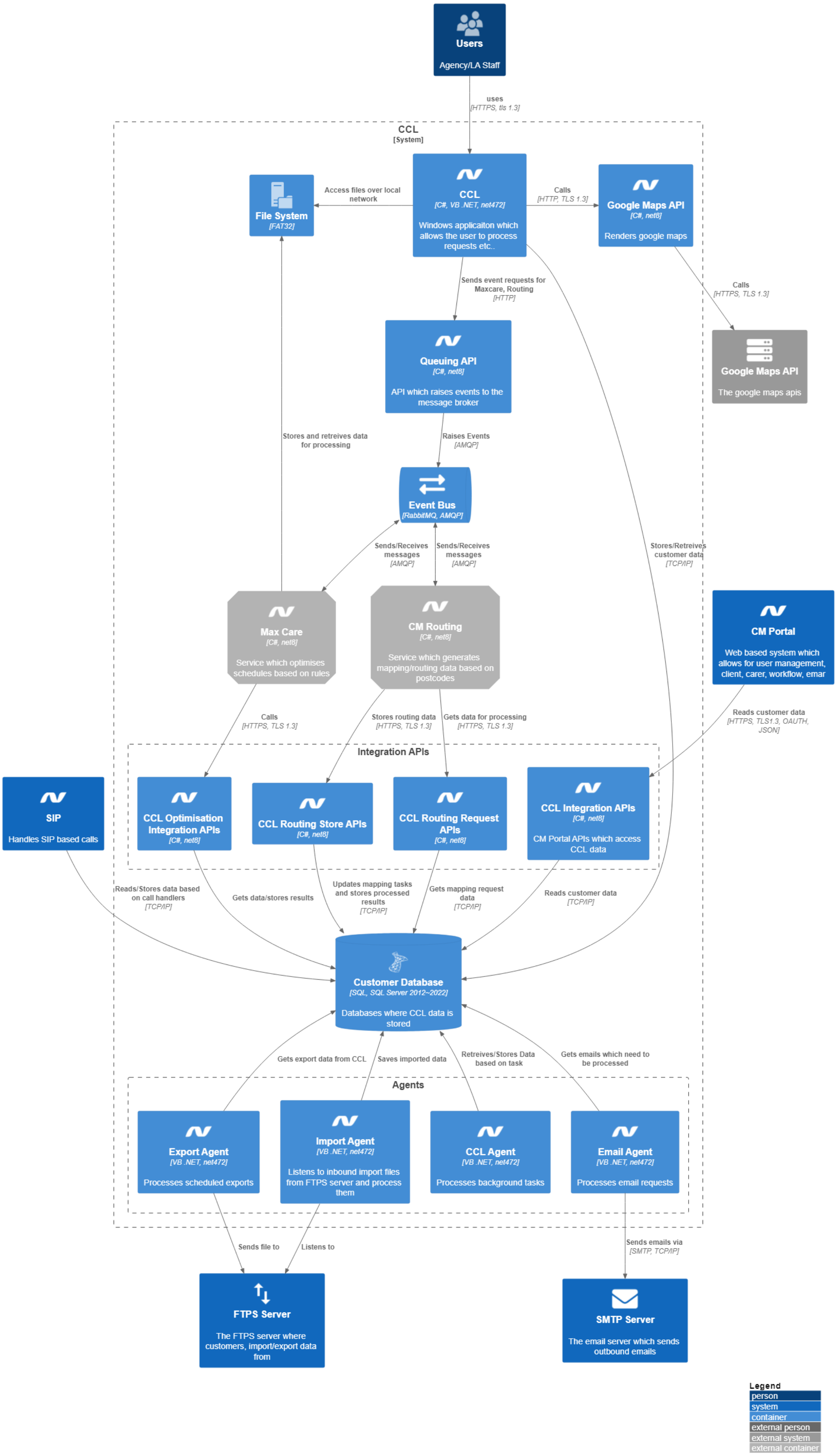
Other set up options available (i.e., isolated/shared)	N/A
Backup details / Storage and Encryption	All backups are stored on disk and are retained for a period of 3 Months. Backups are stored within a multi tenancy data vault and are encrypted at rest. The design of the architecture means that all data is simultaneously available in both the primary datacentre and the secondary datacentre meaning data is always backed up to another geographically diverse site. All Servers are backed up on a daily basis at 10pm. These backups go directly to storage in the DR Datacentre to ensure off-site availability. Backup technology in use is • Veeam • DPM • Commvault
Backups managed by	CE
BCP	ISO 22301
Segregation of Production and Development environments.	Applications are hosted on different VMs/Hosts Database Servers are on different hosts
If there is a web service Is there a mechanism that restricts access to the Web Service	No

About the Mobile App	
Is there a mobile app	Yes – Please see the “Access_CM CM Mobile Fact Sheet” for details on the mobile application
How is data secured between the App & the Server?	
Is Data stored on the device? (If yes, what data? for how long?)	
Format of stored data	
Exit Arrangements	
How is data returned to clients on termination	Self-serve – some clients have a contract clause for us to help if needed. They can use standard reporting tool or our more advanced CMBI tool to extract the data they need.
What is the standard format	csv
How is the data deleted or anonymised	Anonymised as the data model is too complex to delete.

Data Flow / Network Diagram


CCL System Context (High Level)
Users
Agency/LA Staff
accesses via
[https, TLS 1.3]
DC2 CCL!
[Access Data Center]
CM Portal
Web based system which allows for user management, client, carer, workflow, emar
Citrix
Virtual Desktop Host which allows access to CCL! via web browser
federates with
Internal Microsoft Entra
sends mail
[SMTP]
Retreives Data From
[HTTPS, TLS1.3, OAUTH]
Hosts
CallConfirmLive!
The main CCL application which hosts all the features of CCL
Sends emails via
[SMTP, TCP/IP]
SMTP Server
The email server which sends outbound emails
Stores and queries data
[Secure TCP/IP]
Sends/Receives files
[FTPS]
Sends SMS messages via
Customer Databases
Where the customers data is stored
FTPS Server
The FTPS server where customers, import/export data from
SMS System
A system which processes and sends SMS messages
Gets data
[TCP/IP]
Gets data
[TCP/IP]
Sends/Receives files
[FTPS]
Data Warehouse
Collates and processes data for reports and data aggregation
CMBI
Renders customer reports
Customers System
A customers external system which is used to import/export data
Legend
person
system
external person
external system

CCL Diagram - Container



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
Connexica Unit D, Dyson Court Dyson Way Stafford Technology Park Staffordshire ST18 0LQ, United Kingdom	Business Partner	UK	Connexica provide the underlying technology for CMBI. We use Connexica as part of our 3rd line support service so if required they may need to login into a customer's CMBI instance to help solve a problem.	UK	Contract inclusive of GDPR/data privacy provisions
Access Workspace Romania	Affiliate	Romania	Support, onboarding, offboarding and professional services	Romania	Intra-group data processing agreement

Schedule 2 – Processing Activities

This list is non-exhaustive but is intended to describe some of the key processing activities involved in providing the Access Product described in this product fact sheet to you.

For processing activities, we carry out as an independent controller, please see our Privacy Notice.

	Processor	Controller
Onboarding	Activities may include data collection, data manipulation and or upload.	Information pertinent to key persons may be collected and processed by us. For example, a key person for implementation, administrative and/or for financial matters (e.g., payment of invoices).
		All login information to access the product.
BAU	Activities may include the hosting and/or extracting of your data and transferring your data (all or part, as required) to the necessary third parties. Including doing anything with your data which is otherwise necessary to fulfil any professional service requests from you.	Telemetry data and other general product usage data.
		Feedback about the product from end users.
		Processing of any your data through our security defenses (e.g., firewalls).
Support	Activities may include analysing, searching through, or otherwise manipulating and or deleting your data (or part thereof), as per your instruction or as needed to resolve an issue.	Data collected by us using our support platforms, online forms, telephone calls to us etc., pertinent to you raising a support case with us.
Offboarding	Activities may include returning your data or making your data available for download on a self-serve basis and deleting your data.	