



GCI Product/Service	CRM data <i>(this is the personal data of representatives with whom GCI interacts for marketing and customer relationship purposes)</i>	User Data <i>(this is focussed on a customer's end users e.g. their contact details and authentication details, among other things)</i>	Communications Data <i>(this will include a range of traffic and location data that GCI will process in order to perform certain services (e.g. number called, date/time, duration of call))</i>	Content Data <i>(this would cover a range of data that is processed in the provision of GCI's services but which is created by users – ranging from video, call and email content data)</i>	Other (incl Sensitive Data)	Non-EEA Processing of Customer Data by GCI as Processor	Additional Info
<b>Web Hosting</b>	<b>C</b> Personal contact details for key account contacts. Customer billing and service data.	<b>P</b> Personal contact details for key account contacts. Customer administrators' name.	N/A	<b>P</b> Customer data will be hosted on GCI infrastructure and may include personal data e.g. web-users	<b>P Sensitive data:</b> Individuals may share their sensitive personal data or about other users in the form of Content Data which GCI employees may have access to in hosting the website or in providing support, but it is not required or requested by GCI to perform the services.	N/A	Note that support service requests are managed using ServiceNow (in the EEA). Cpanel is hosted on Microsoft cloud infrastructure - note that Microsoft is EU/US Privacy Shield certified and utilises EC Standard Contractual C+H5lauses.
<b>VMCS (Virtual Machine Continuity Software)</b>	<b>C</b> Customer contact details for services Customer billing and service data.	<b>P</b> Any customer user data is potentially visible to internal administrators.	N/A	<b>P</b> All customer restores/accesses i.e. any files which are backed-up/restored using VMCS and which contain personal data.	<b>P Sensitive data:</b> Individuals may share their sensitive personal data or personal data about other users when making use of the services to which GCI provide support. This would be in the form of Content Data which GCI employees may have access to / visibility of during a the back-up/recovery process or a troubleshooting engagement, but it is not routinely collected or requested by GCI to perform the services.	N/A	Note that support service requests are managed using ServiceNow (in the EEA). Zerto provides applications which are utilised by GCI and held on GCI infrastructure to orchestrate VMCS services. No support services are provided by Zerto and Zerto will not have access to GCI customer data.
<b>SecureVault</b>	<b>C</b> Personal contact details	<b>P</b> User portal account names in format email address or group account, e.g.,	N/A	<b>P</b> All customer restores/accesses i.e.	<b>P Sensitive data:</b> Individuals may share	N/A	Note that support service requests are managed using



	for services. Customer billing and service data.	support@xyz.com. Any customer user data is potentially visible to internal administrators.		any files which are backed-up/restored using GCI SecureVault and which contain personal data.	their sensitive personal data or personal data about other users when making use of the services to which GCI provide support. This would be in the form of Content Data which GCI employees may have access to / visibility of during a the back-up/recovery process or a troubleshooting engagement, but it is not routinely collected or requested by GCI to perform the services.		ServiceNow (in the EEA).
<b>Public Cloud</b>	<b>C</b> Personal contact details for services. Customer billing and service data.	<b>P</b> Personal contact details for key account contacts  Customer administrators' name Customer administrators' account log-on (e.g. e-mail address or Live ID)	N/A	<b>P</b> GCI would only have access to content data in the provision of 1st and 2nd line support (GCI public cloud does not host the customer's data on GCI infrastructure, this is provided by Microsoft Azure).	<b>P Sensitive data:</b> Individuals may share their sensitive personal data or personal data about other users when making use of the services to which GCI provide support. This would be in the form of Content Data which GCI employees may have access to / visibility of during a troubleshooting engagement, but it is not routinely collected or requested by GCI to perform the services.	N/A	Note that support service requests are managed using ServiceNow (in the EEA). Customer data is processed in Microsoft Azure and customer will select regions in which their data will be hosted by Microsoft (note that Microsoft is EU/US privacy shield certified and utilises the EC's Standard C+H15ontractual Clauses).
<b>Private Cloud</b>	<b>C</b> Customer billing and service data Customer contact details GCI email system.	<b>P</b> Personal contact details for key account contacts Customer administrators' name Customer administrators' account log-on (e.g. e-mail address)	<b>P</b> IP addresses in ServiceNow for the provision of support services.	<b>P</b> All customer data is stored on GCI infrastructure including files containing personal data.	<b>P Sensitive data:</b> Individuals may share their sensitive personal data or personal data about other users when making use of the services to which GCI provide support. This would be in the form	N/A	Note that support service requests are managed using ServiceNow (in the EEA). Customer portal uses the V-cloud direct portal which is hosted on GCI's UK infrastructure.



					of Content Data which GCI employees may have access to / visibility of during a troubleshooting engagement, but it is not required or requested by GCI to perform the services.		
<b>Managed Services</b>	<b>C</b> Personal contact details of customer representatives, including: Users Name, Email Address, Telephone Number, Site Address, Job Title	<b>P</b> User data held to support incident/problem/change includes: Name, job title, email, business phone number, mobile phone number, site address, reporting line. In the context of an incident, may record: MAC address, IP address, machine name etc	<b>P</b> Only in exceptional circumstances where Customer may provide access to Communications Data for troubleshooting purposes	<b>P</b> Content Data generated by end users may be uploaded to ServiceNow / sent to an assigned engineer during troubleshooting which may contain personal data. This can take many forms including screenshots / email / instant message conversations etc.	<b>P</b> <b>Sensitive data:</b> Individuals may share their sensitive personal data or personal data about other users when making use of the services to which GCI provide support. This would be in the form of Content Data which GCI employees may have access to / visibility of during a troubleshooting engagement, but it is not routinely collected or requested by GCI to perform the services.	N/A	Note that support service requests are managed using ServiceNow (in the EEA).
<b>Flexible Support</b>	<b>C</b> Personal contact details of customer representatives, including: Users Name, Email Address, Telephone Number, Site Address, Job Title	<b>P</b> User data held to support incident/problem/change includes: Name, job title, email, business phone number, mobile phone number, site address, reporting line. In the context of an incident, may record: MAC address, IP address, machine name etc	<b>P</b> Only in exceptional circumstances where Customer may provide access to Communications Data for troubleshooting purposes	<b>P</b> Content data may be generated by end users and uploaded to ServiceNow / sent to an assigned engineer during troubleshooting which contains personal data. This can take many forms including screenshots / email / instant message conversations etc.	<b>P</b> <b>Sensitive data:</b> Individuals may share their sensitive personal data or personal data about other users when making use of the services to which GCI provide support. This would be in the form of Content Data which GCI employees may have access to / visibility of during a troubleshooting engagement, but it is not routinely collected or requested by GCI to perform the services.	N/A	Note that support service requests are managed using ServiceNow (in the EEA).



<b>Contact Centre</b>	<b>C</b> Customer and supplier representatives' Name, Email Address, Telephone number, Site address, Job title, [User screen shot,] Contact history	<b>P</b> [Name, Job Title, Email , Phone, Location, Reporting Line, Call Quality , IP Address, MAC address, Call History/Log Details, Agent Skills, Hold location data and map address for emergency/number contact]	<b>P</b> [Name, Job Title, Email , Phone, Location, Reporting Line, Call Quality , IP Address, MAC address, Call History/Log Details, Agent Skills, Hold location data and map address for emergency/number contact]	<b>P</b> Historic interaction data. Agent interaction times and functions recorded against activity. Any data which is inputted into/recorded by the contact centre solution when used by a client's personnel.	<b>C</b> Network monitoring/routing info for the purpose of monitoring the GCI contact centre server.  <b>P</b> <b>Sensitive data:</b> users may elect to share sensitive personal data when using GCI services but GCI does not require or request sensitive data to provide the services.	Support may be provided by Enghouse in New Zealand if vendor support is required [note that New Zealand has a European Commission adequacy decision]	GCI Contact Centre is an Enghouse product. Enghouse is a GCI sub-processor when it provides support services(level 3/4) and software fixes for the GCI Contract Centre product. GCI's contact centre solution is integrated with other GCI products and services - where this is the case, please review the information in this table for other relevant GCI products and services. Where contact centre is installed on the client's infrastructure rather than on GCI's cloud infrastructure, GCI's processing of personal data will be limited (e.g. to support services).
<b>Co-Location</b>	<b>C</b> Customer billing and service data Personal contact details for key account contacts	<b>P</b> Personal contact details for customer key account contacts/administrators	N/A	N/A	No sensitive data	N/A	GCI's co-location services involve the housing of customer's hardware in GCI's premises but without any physical or logical access rights. As such, GCI processes very little customer personal data in the provision of co-location services.
<b>Cloud Workspace (Managed Virtual Desktop)</b>	<b>C</b> Customer billing and service data Personal contact details for key account contacts	<b>P</b> End user account names in format firstname.lastname@business Customer administrators' account log-on in format firstname.lastname@business. Any customer user data which is held in the solution is potentially visible to a GCI administrator.	N/A	<b>P</b> Any records containing personal data will be hosted on GCI infrastructure.	<b>P</b> <b>Sensitive data:</b> Individuals may share their sensitive personal data or personal data about other users when making use of the services to which GCI provide support. This would be in the form of Content Data which GCI employees may have access to	N/A	N/A



					in hosting customer's data or in providing support, but it is not required or requested by GCI to perform the services.		
<b>Call Recording</b>	<b>C</b> Name, Contact details (e.g. SfB IM Address, Tel no), Job title[, User screen shot,] Contact history	<b>P</b> Name, Job Title, SfB Phone, Reporting Line, Call Quality, IP Address, MAC address, Call History/Log Details	<b>P</b> [[IP Address, MAC address,] Call History/Log Details - caller/called party data and video recording and screen recording meta-data.	<b>P</b> Interactions between individuals including IM, skype calls, video recording and screen recording.	<b>C</b> Network monitoring/routing info for the purpose of monitoring the GCI call recording server.  <b>P</b> <b>Sensitive data:</b> users may elect to share sensitive personal data when using GCI services but GCI does not require or request sensitive data to provide the services.	N/A	GCI call recording is a Verba/Verint solution which is implemented and supported by GCI. Verba/Verint is a GCI sub-processor when it provides support services(level 3/4) and software fixes for the GCI call recording product. GCI's call recording solution is integrated with other GCI products and services - where this is the case, client's should review the information in this table for those other integrated GCI products and services which it has purchased from GCI.
<b>Managed Firewall</b>	<b>C</b> Personal contact details of customer and supplier representatives, including: Users Name, Email Address, Telephone Number, Site Address , Job Title	<b>P</b> Users Name, IP Address, Device ID, MAC Address	<b>P</b> Details of traffic transmitted via the firewall are likely to be recorded on the device and stored for a varying length of time (dependent on customer preference and configuration). This metadata includes date / time information and is stored within the system to support troubleshooting in the event of issues with the service, or investigation in to network activity. This metadata includes elements of personal data including: IP Address, Device ID, Routing Information,	<b>P</b> Content data may be generated by end users and transmitted by users of the service. In most cases the data simply passes through the system, however where UTM functionality is used and the data falls within the scope of a defined policy the data may be stored on the device for auditing purposes.	<b>P</b> <b>Sensitive data:</b> not actively processed but individuals may share their own sensitive personal data, or that of others over the internet which will transit the Managed Firewall. In the event that this data triggers a UTM policy intended to prevent the transmission of that data, the relevant data may be recorded within device logs for audit purposes.  In the case of internet access, the Managed Firewall service has	N/A	GCI's managed firewall solution is integrated with other GCI products and services (e.g. GCI managed services) - where this is the case, please review the information in this table for other relevant GCI products and services. Data may be processed in Vodafone datacentres (within the EEA).



			Source / Destination IP addresses visited		the ability to restrict, or record user activity which may include sensitive personal data. GCI does not request or require the provision of sensitive personal data to provide the managed firewall service.		
<b>SecureMail Email Security</b>	<b>C</b> Personal contact details of customer representatives, including: Users Name, Email Address, Telephone Number, Site Address , Job Title	<b>P</b> Email address/user account	<b>P</b> Details of emails sent to / from a given email address are recorded by the SecureMail service. This metadata includes date / time information and is stored within the system to support troubleshooting in the event of issues with the service, or investigation in to network activity. This metadata includes : IP Address, Device ID, Routing Information, Source / Destination IP addresses visited	<b>P</b> Content data may be generated by end users and transmitted by users of the service. In most cases the data simply passes through the system, however where certain thresholds are reached an email may be quarantined within the system until reviewed by the end user concerned, or an administrator.	<b>P</b> <b>Sensitive data:</b> individuals may share their sensitive personal data or personal data within emails which are subsequently quarantined by the service. This would be in the form of Content Data which GCI employees may have access to / visibility of during a troubleshooting engagement. Sensitive personal data is not requested or required by GCI to provide the SecureMail Email Security service.	N/A	Data may be processed in Vodafone datacentres (within the EEA).
<b>Skype for Business On-Premise</b>	<b>C</b> Users Name, Email Address, Telephone number, Site address, Job title, User screenshot, survey responses	<b>P</b> Name, Job Title, Email, Phone, Location, Reporting Line, Call Quality, IP Address, MAC address, Call History/Log Details, Types of calls i.e. IM/Call/Conference  Hold location data and map address for emergency/number service (network map) Optional: For all customers hold IP address/MOS. This is optional (90 days) default. <b>This information would only be processed by GCI in the provision of support services.</b>	<b>P</b> Call Quality, IP Address, MAC address, Call History/Log Details, Types of calls i.e. IM/Call/Conference  Hold location data and map address for emergency/number service (network map) Optional: For all customers hold IP address/MOS. This is optional (90 days) default. <b>This information would only be processed by</b>	<b>P</b> IM conversations and calls – recording and archive *Note: for Videos this is a local PC user copy - <b>this information would only be processed by GCI in the provision of support services.</b>	<b>P</b> <b>Sensitive data:</b> individual users but users may share their sensitive personal data or personal data about other users when making use of the services but it is not required or requested by GCI to provide SfB on-premise solution and <b>this information would only be processed by GCI in the provision of support services.</b>	N/A	SfB On-Premise is configured by the customer and runs on the customer's infrastructure. GCI has very limited access to customer personal data and this would be limited to the provision of support services where the customer provides access to its SfB deployment, in which case, the information set out in this row may be made available to GCI. <b>Outside of this, GCI will not process the</b>



			<b>GCI in the provision of support services.</b>				<b>data in this row.</b> GCI's SfB on-premise solution is integrated with other GCI products and services - where this is the case, please review the information in this table for other relevant GCI products and services. Support tickets are managed using AutoTask (in the EEA).
<b>SIP Trunks</b>	<b>C</b> Customer Name, Contact Name, Email Address, Tel no, Job title, Address, Complaints.	<b>P</b> End user email address	<b>P</b> IP Address, Call routing information, Call History/Log Details, Caller ID Info	N/A	<b>C</b> <b>Monitoring:</b> GCI monitor the status of the SIP trunk connection to check if it is available.  No sensitive data	N/A	Support tickets are managed using AutoTask (in the EEA).
<b>Skype for Business Hosted</b>	<b>C</b> Users Name, Email Address, Telephone number, Site address, Job title, User screenshot, survey responses	<b>P</b> Name, Job Title, Email, Phone, Location, Reporting Line, Call Quality, IP Address, MAC address, Call History/Log Details, Types of calls i.e. IM/Call/Conference  Hold location data and map address for emergency/number service (network map) Optional: For all customers hold IP address/MOS. This is optional (90 days) default.	<b>P</b> Call Quality, IP Address, MAC address, Call History/Log Details, Types of calls i.e. IM/Call/Conference  Hold location data and map address for emergency/number service (network map) Optional: For all customers hold IP address/MOS. This is optional (90 days) default.	<b>P</b> IM conversations and calls – recording and archive *Note: for Videos this is a local PC user copy	<b>C</b> Network monitoring/routing info - GCI monitor the server not customers activity/user data. <b>P</b> <b>Sensitive data:</b> users may share their sensitive personal data or personal data about other users when making use of the services but this is not required or requested by GCI to provide the service.	N/A	Support tickets are managed using AutoTask (in the EEA). GCI's SfB on-premise solution is integrated with other GCI products and services - where this is the case, please review the information in this table for other relevant GCI products and services.
<b>UC Analytics</b>	<b>C</b> Customer's representatives Name, Email Address, Tel no, Site location, Job title, User screen shot, survey responses	<b>P</b> Name, Job Title, Email, Phone, Location, Reporting Line, Call Quality, IP Address, MAC address, Call History/Log Details, Types of calls i.e. IM/Call/Conference	<b>P</b> Call Quality, IP Address, MAC address, Call History/Log Details, Types of calls i.e. IM/Call/Conference	N/A	No sensitive data	UC may provide support services from Romania.	UC Analytics is provided by Code Software - it is possible that personal data would be shared with Code (in the EEA) in the event of a support issue which could not be resolved by GCI.
<b>Microsoft Office 365</b>	<b>C</b> Users Name, Email Address,	<b>P</b> Name, Job Title, Email, Phone, Location, Reporting Line, Call Quality,	N/A	N/A	No sensitive data	N/A [note that Microsoft may process	GCI is a reseller of Microsoft Office 365 products and proceses



	Tel no, Site location, Job title, User screen shot, Survey responses	IP Address, MAC address, Microsoft Tenant ID				customer data on infrastructure outside the EEA - Microsoft is EU/US Privacy Shield certified and will enter into a form of European Commission Standard Contractual Clauses with its customers]	a limited amount of customer information as the product/service is provided by Microsoft and customer data is hosted on Microsoft infrastructure. Support tickets are managed using AutoTask (in the EEA).
<b>Non-Geo Numbers</b>	<b>C</b> Customer Name, Contact Name, Email Address, Tel no, Job title, Address, Complaints.	<b>P</b> End-user e-mail addresses	<b>P</b> IP address, call routing information, call history/log details, caller and called party data	N/A	<b>C</b> <b>Monitoring:</b> GCI only monitor the status of the SIP trunk connection to check if it is available.  No sensitive data	N/A	Support tickets are managed using AutoTask (in the EEA).
<b>Hosted Antivirus</b>	<b>C</b> Users Name, Email Address, Telephone Number, Site Address, Job Title	<b>P</b> Username, Device Name, IP Address, Mac Address, Websites Visited & administrator user account information	N/A	<b>P</b> Content Data would only be reviewed in the course of providing troubleshooting services by GCI's service desk during which this data may be accessed/viewed.	<b>P</b> <b>Sensitive data:</b> Individuals may share their sensitive personal data or personal data about other users when making use of the services to which GCI provide support. This would be in the form of Content Data which GCI employees may have access to / visibility of during deployment or a troubleshooting engagement, but it is not routinely collected or requested by GCI to perform the services.	In exceptional circumstances if a support issue cannot be resolved by GCI and Kaspersky in the EEA it is possible that the issue may be escalated to Kaspersky in Russia.	Note that support service requests are managed using ServiceNow (in the EEA) and some data may be held in Vodafone's data centres (in the EEA). Support issues may be escalated to Kaspersky for support (within the EEA), in exceptional circumstances an issue may be escalated to Kaspersky in Russia.
<b>Enterprise Mobility + Security</b>	<b>C</b> Customer billing and service data	<b>P</b> Personal contact details for key account contacts Customer administrators' name	N/A	<b>P</b> GCI's deployment and support teams have the ability to see and access any data and settings held within a customer's Microsoft tenancy during deployment/support.	<b>P</b> <b>Sensitive data:</b> Individuals may share their sensitive personal data or personal data about other users when making use of the	N/A	Note that support service requests are managed using Autotask (in the EEA). Data is held in Microsoft data centres with region selected by the customer - note



					services to which GCI provide support. This would be in the form of Content Data which GCI employees may have access to / visibility of during deployment or a troubleshooting engagement, but it is not routinely collected or requested by GCI to perform the services.		that Microsoft is EU/US Privacy Shield certified and utilises EC Standard Contractual Clauses.
<b>Mandarine Academy Learning Platform</b>	<b>C</b> Users Name, Email Address, Tel no, Site location, Job title, User screen shot	<b>P</b> Name, Job Title, Email, Phone	N/A	N/A	No sensitive data	N/A	Support tickets are managed using AutoTask (in the EEA).
<b>Datto SIRIS ALTO Server and Data Protection</b>	<b>C</b> Customer billing and service data Personal contact details for key account contacts	<b>P</b> Any customer user data is potentially visible to internal administrators.	N/A	<b>P</b> Any customer content data is potentially visible to internal administrators.	<b>P Sensitive data:</b> Individuals may share their sensitive personal data or personal data about other users when making use of the services to which GCI provide support. This would be in the form of Content Data which GCI employees may have access to / visibility of during deployment or a troubleshooting engagement, but it is not routinely collected or requested by GCI to perform the services.	N/A	Note that support service requests are managed using ServiceNow (in the EEA). Software vendor is Datto. Datto software is held on GCI infrastructure. No support services are provided by Datto. Datto may store back-ups of customer data at their EEA data centres depending on whether the customer elects to use GCI or Datto infrastructure.
<b>Vaeem Cloud Connect</b>	<b>C</b> Customer billing and service data Personal contact details for key account contacts	N/A	N/A	<b>P</b> Any customer data is potentially visible to internal administrators (but GCI would need to request Veeam to provide access to the data). A service desk engineer	<b>P Sensitive data:</b> Individuals may share their sensitive personal data or personal data about other users when making use of the services to which GCI	N/A	Note that support service requests are managed using ServiceNow (in the EEA). Software vendor is Vaeem. Vaeem software is hosted on GCI infrastructure. No support services are



				could log into the customers environment and initiate a restore.	provide support. This would be in the form of Content Data which GCI employees may have access to / visibility of during deployment or a troubleshooting engagement, but it is not routinely collected or requested by GCI to perform the services.		provided by Vaeem and Vaeem will not have access to GCI customer data.
<b>Hosted SMS</b>	<b>C</b> Customer Name, Contact Name, Email Address, Tel no, Job title, Address	<b>P</b> Name, Email address, MD5 Hashed password, photo	<b>P</b> Recipients mobile number, IP Address is logged for API connections, MAC and device ID if available, Message routing information, Recipient message History/Log Details	<b>P</b> Message content	<b>P</b> <b>Sensitive data:</b> The customer has control over the content of the messages and may elect to include sensitive data.	N/A	Support tickets are managed using AutoTask (in the EEA). SMS messages are sent via mobile networks (e.g. Vodafone, EE, O2) and SMSC aggregator (CLX Communications)
<b>Contact Centre (EICC)</b>	<b>C</b> Users Name, Email Address, Tel no, Site location, Job title, User screen shot, Contact history, surveys.	<b>P</b> [Name, Job Title, Email, Phone, Location, Reporting Line, Call Quality, IP Address, MAC address, Call History/Log Details, Agent Profile & Skills, Hold location data and map address for emergency/number contact]	<b>P</b> [Name, Job Title, Email, Phone, Location, Reporting Line, Call Quality, IP Address, MAC address, Call History/Log Details, Agent Skills, Hold location data and map address for emergency/number contact. Agent interaction times and functions recorded against activity.]	<b>P</b> [Interaction data i.e. records of interactions between customer's staff and other individuals using the contact centre (EICC) product including IM, call recording, video recording and screen recording.]	Network monitoring/routing info for the purpose of monitoring the GCI contact centre server.  <b>Sensitive data:</b> users may elect to share sensitive personal data when using GCI services but GCI does not require or request sensitive data to provide the services.	Support may be provided by Enghouse in New Zealand if vendor support is required [note that New Zealand has a European Commission adequacy decision]	GCI Contact Centre is an Enghouse product. Enghouse is a GCI sub-processor when it provides support services(level 3/4) and software fixes for the GCI Contract Centre product. GCI's contact centre solution is integrated with other GCI products and services - where this is the case, client's should review the information in this table for those other integrated GCI products and services which it has purchased from GCI. Where contact centre is installed on the client's infrastructure rather than on GCI's cloud infrastructure, GCI's processing of personal data will be limited (e.g. to support services).



<b>PCI DSS Hosted Solution</b>	<b>C</b> [Customer Name, Contact Name, Email Address, Telephone number, Job title, Address]	<b>[N/A - where GCI processes information about contact centre agents for customers who also purchase GCI's PCI solution, agent details processed by GCI are captured in the 'contact centre' product entries - see 'additional info']</b>	<b>[N/A - see Additional Info]</b>	<b>[N/A - see Additional Info]</b>	No sensitive data is collected or processed in respect of the PCI product.	N/A	GCI PCI solution is a C3 product. No personal data is held in the PCI solution and any personal data surrounding the payment card authorisation process would be processed by other solutions e.g. GCI call recording (but payment card authorisation process would be suppressed), GCI contact centre of Skype for Business. Please see the separate entries in this table for details.
<b>Managed SMS Gateway</b>	<b>C</b> Customer Name, Contact Name, Email Address, Telephone number, Job title, Address	<b>P</b> Name, Email address, MD5 hashed password [only where GCI provide managed services and the client uses the Poller database]	<b>P</b> Recipients mobile number and message content data, CDRs, IP Address is stored for Poller access and remote support, Apache server logs IP address, MAC and device ID if available, Message routing information, Recipient message History/Log Details	<b>P</b> Message content data	<b>P/C</b> Gateway IP address and Customer LAN. Used for status monitoring ( <b>C</b> ) and remote support ( <b>P</b> ).  <b>Sensitive data:</b> users may share their sensitive personal data or personal data about other users when making use of the services but this is not required or requested by GCI to provide the service.	Support may be provided by hardware vendor, Hypermedia in Israel, if 3rd level support is required [note that Israel has a European Commission adequacy decision]	Messages are sent over telecoms networks (e.g. EE, Vodafone). SIM cards will be delivered to GCI customers by third party vendors - 2 Circles, The Phone Shop, DuoCall and Connect Telecom. Support tickets are managed using AutoTask (in the EEA).
<b>Managed GSM Gateway</b>	<b>C</b> Customer Name, Contact Name, Email Address, Telephone number, Job title, Address	<b>P</b> Name, Email address, MD5 hashed password [only where GCI provide managed services and the client uses the Poller database]	<b>P</b> IP Address is stored for Poller access and remote support, Apache server logs IP address, MAC and device ID if available, Call routing information, Call History/Log Details, Recipient number data	<b>P</b> N/A	<b>P/C</b> Gateway IP address. Used for status monitoring ( <b>C</b> ) and remote support ( <b>P</b> ).  No sensitive data	Support may be provided by hardware vendor, Hypermedia in Israel, if 3rd level support is required [note that Israel has a European Commission adequacy decision]	Support tickets are managed using AutoTask (in the EEA). CLI data is sent to telecoms networks to route the call (e.g. EE, Vodafone). SIM cards will be delivered to GCI customers by third party vendors - 2 Circles, The Phone Shop, DuoCall and Connect Telecom. Support tickets are managed using AutoTask (in the EEA).



<b>Network Monitoring</b>	<b>C</b> Users Name, Email Address, Telephone number, Site location, Job title	<b>P</b> Name, Job Title, User Name, Password, Email, Phone, Location, IP Address, MAC address, Ticket History/Log Details	N/A	N/A	<b>C</b> GCI monitor the network for utilisation and packet loss statistics including network devices	Support may be provided by hardware vendor, Hypermedia in Israel, if 3rd level support is required [note that Israel has a European Commission adequacy decision]	Support tickets are managed using AutoTask, ServiceNow and Supportworks (in the EEA). GCI resells Hortium's monitoring software - Hortium may be engaged to provide higher level support.
<b>MPLS</b>	<b>C</b> Users Name, Email Address, Tel no, Site location, Job title	<b>P</b> Name, Job Title, Email, Phone, Location, IP Address, MAC address, Ticket History/Log Details	<b>P</b> IP Address MAC address	N/A	<b>C</b> GCI monitor the network for utilisation and packet loss statistics including network devices  No sensitive data	N/A	Support tickets are managed using AutoTask (in the EEA). Customer contact details may be shared with MPSI for customer site visits, Virgin Media Business, Talk Talk Business and BT Wholesale as the connectivity providers, Hortium as the vendor of the monitoring software and for support requests.
<b>DIA Services</b>	<b>C</b> Users Name, Email Address, Tel no, Site location, Job title	<b>P</b> Name, Job Title, Email, Phone, Location, IP Address, MAC address, Ticket History/Log Details	<b>P</b> IP Address MAC address when using NAT, originators private IP address can be obtained	N/A	<b>C</b> GCI monitor the network for utilisation and packet loss statistics including network devices  No sensitive data	N/A	Support tickets are managed using AutoTask, ServiceNow and Supportworks (in the EEA). Customer contact details may be shared with MPSI for customer site visits, Virgin Media Business, Talk Talk Business and BT Wholesale as the connectivity providers, Hortium as the vendor of the monitoring software and for support requests.
<b>DDoS Protection</b>	<b>C</b> Users Name, Email Address, Telephone number, Site location, Job title	<b>P</b> Email Address, Name, Telephone Number	<b>P</b> Metadata relating to actual or suspected attacks will be recorded by the service. This metadata includes date / time information and is stored within the system for reporting	<b>P</b> E-mail content - GCI's DDoS service is focused on the protection of inbound data paths. All traffic is redirected via GCI's data-centres to support the removal of bad traffic based on	<b>C</b> The service is predicated on GCI control and manipulation of network routing (which would be known via provision of Network Services,	N/A	Note that support service requests are managed using ServiceNow (in the EEA). Support tickets are managed using AutoTask (in the EEA).



			and support purposes. This metadata is likely to include elements of personal data including: IP Address Device ID Routing Information	packet / pattern sequences. This is achieved through comparison with known attack profiles. Data is not retained by the service. "Bad" data is dropped, and statistics relating to the volume and type(s) of traffic are recorded for reporting purposes. The service manages data in transit rather than files and access to content data is unlikely.	governed by a separate GDPR mapping document). <b>P Sensitive Data:</b> GCI does not require or request any sensitive personal data to provide the service, but sensitive personal data may be contained in the customer's content data.		
<b>Network WLAN Service</b>	<b>C</b> Users Name, Email Address, Tel no, Site location, Job title, survey responses	<b>P</b> Name, Job Title, Email, Phone, Location, IP Address, MAC address, Ticket History/Log Details	<b>P</b> IP Address MAC address Browsing history by MAC/IP address is available to the customer as well as location of these within a building where the WLAN is available.	<b>N/A</b> The customer can send any data they wish to over this service and GCI doesn't control or have visibility of it	<b>C</b> GCI GCI monitor the network for utilisation and packet loss statistics including network devices  No sensitive data	N/A	Support tickets are managed using AutoTask (in the EEA). Customer contact details may be shared with MDSI for customer site visits. Aruba Central stores IP and MAC address information in AWS in Europe. GCI resells the HPE Aruba products.
<b>Network LAN Service</b>	<b>C</b> Users Name, Email Address, Tel no, Site location, Job title, survey responses	<b>P</b> Name, Job Title, Email, Phone, Location, IP Address, MAC address, Ticket History/Log Details	<b>P</b> IP Address MAC address Browsing history by MAC/IP address is available to the customer as well as location of these within a building where the WLAN is available.	<b>N/A</b> The customer can send any data they wish to over this service and GCI doesn't control or have visibility of it	<b>C</b> GCI monitor the network for utilisation and packet loss statistics including network devices  No sensitive data	N/A	Support tickets are managed using AutoTask (in the EEA). Customer contact details may be shared with MDSI for customer site visits. Aruba Central stores IP and MAC address information in AWS in Europe. GCI resells the HPE Aruba products.
<b>UC:SfB - Cloud PBX</b>	<b>C</b> Users Name, Email Address, Tel no, Site location, Job title, User screen shot, survey responses	<b>P</b> [Name, Job Title, Email, Phone, Location, Reporting Line, Call Quality, IP Address, MAC address, Call History/Log Details, Types of calls i.e. IM/Call/Conference Hold location data and map address for emergency/number service (network map) Optional: For all customers hold IP	<b>P</b> SIP/PTSN call data passes through GCI's Cloud Connector Edition server and call information is stored in CDRs.	N/A	No sensitive data.	N/A	Support tickets are managed using AutoTask (in the EEA).



		address/MOS. This is optional (90 days) default.]					
<b>UC: Survival Branch Appliance</b>	<b>C</b> Users Name, Email Address, Tel no, Site location, Job title, User screen shot, survey responses	<b>P</b> Name, Job Title, Email, Phone, Location, Reporting Line, Call Quality, IP Address, MAC address, Call History/Log Details, Types of calls i.e. IM/Call/Conference Hold location data and map address for emergency/number service (network map) Optional: For all customers hold IP address/MOS. This is optional (90 days) default.	<b>P</b> When providing maintenance support remotely, GCI may have access to some traffic data or IP addresses. Call data recorded and passed to local SGL database. Configured centrally on Skype for Business and not generally accessed by GCI (only in exceptional circumstances i.e. provision of support services)	N/A	<b>C</b> Network monitoring/routing info GCI monitors the server and does not monitor customers activity/user data.  No sensitive data	N/A	SBA is an on-premise solution and GCI would have limited access to any personal data which is processed by the SBA hardware - this would be limited to access in the event of a support issue. GCI's SBA solution is integrated with other GCI products and services - where this is the case, client's should review the information in this table for those other integrated GCI products and services which it has purchased from GCI. Support tickets are managed using AutoTask (in the EEA).
<b>UC: Multi Tenant Lync</b>	<b>C</b> Users Name, Email Address, Tel no, Site location, Job title, User screen shot, survey responses	<b>P</b> Name, Job Title, Email, Phone, Location, Reporting Line, Call Quality, IP Address, MAC address, Call History/Log Details, Types of calls i.e. IM/Call/Conference Hold location data and map address for emergency/number service (network map) Optional: For all customers hold IP address/MOS. This is optional (90 days) default.	<b>P</b> Call Quality, IP Address, MAC address, Call History/Log Details, Types of calls i.e. IM/Call/Conference Hold location data and map address for emergency/number service (network map) Optional: For all customers hold IP address/MOS. This is optional (90 days) default.	<b>P</b> IM conversations and calls – recording and archive *Note: for Videos this is a local PC user copy	<b>C</b> Network monitoring/routing info GCI monitor the server not customers activity/user data.  <b>P</b> <b>Sensitive Data:</b> GCI does not require or request any sensitive personal data to provide the service, but sensitive personal data may be contained in the customer's content data.	N/A	Support tickets are managed using AutoTask (in the EEA).
<b>Rapid Deployment</b>	<b>C</b> Customer Name, Contact Name, Email Address, Tel no, Job title, Address, details of complaints.	<b>P</b> Contact Name, Business address, Email address, Contact number, Ticket History / Log Details	<b>P</b> Data usage (CDRs) IP Address is stored for remote management and support. Data routing information, Usage History / Log Details,	N/A	<b>C/P</b> CPE IP address is used for status monitoring(C) and remote support and management (P). No sensitive data.	N/A	CPE management portal and comms portal is provided by Comms365 and will also provide 3rd line support [within the EEA]. Support tickets are managed using



			Data routing information				AutoTask (in the EEA). Customer contact information may be provided to third party hardware suppliers to delivery replacement hardware. Data is transferred over mobile networks e.g. Vodafone, EE, O2.
<b>Alcatel PBX</b>	<b>C</b> Customer Name, Contact Name, Email Address, Tel no, Job title, Address, details of complaints	<b>P</b> Name, Job Title, Email, Phone number, Extension number, Handset IP Address for Support purposes, Handset MAC address for Support purposes, Call History/Log Details	<b>P</b> IP Address MAC address Call History/Log Details	<b>P</b> Call recording and archive* *Note: Stored on external device – GCI have no access to this.	<b>C</b> Network monitoring  No sensitive data	Customer data may be processed by Alcatel Lucent outside the EEA when providing support services for the Alcatel PBX solution.	Alcatel PBX is an on-premise solution and limited customer personal data is processed by GCI as customer personal data is held locally by each customer. Support Works is used to manage support requests. Customer personal data may be shared with Alcatel Lucent for support purposes. Customer information may be provided to third parties for delivery of hardware to customer premises. Customer address/contact details will be provided to BT/Gamma for service provision (PSTN/Broadband)
<b>Broadsoft Hosted Voice</b>	<b>C</b> Customer Name, Contact Name, Email Address, Tel no, Job title, Address, details of complaints	<b>P</b> Name, Email address, Address, DDI, MAC Address Ticket History / Log Details Call History / Log details	<b>P</b> Recipient number data, Device IP is displayed in the Management Portal but not stored. Device MAC address is stored for configuration. Call routing information via CDR. Call History/Log Details	<b>P</b> Call-recordings - only in the event that support is requested and this information is made available/accessed by GCI for this purpose.	No sensitive data	N/A	Customer data is stored on the Broadsoft Management Portal which is managed and hosted by BT (within the EEA) and accessible by the customer. CLI information is also transmitted to BT in order to route the call. GCI would not have access to the portal other than for support purposes. Customer details may also be shared with BT for



							support requests. Customer support requests are managed using AutoTask (within the EEA).
--	--	--	--	--	--	--	--