

## **Product Privacy Information**

December 2019

Certain services provided by Gamma (as defined below) require Gamma to process personal data on behalf of the customer (“**Product Related Personal Data**”). In relation to such processing Gamma is the processor and the customer is the controller.

### **Contact Details**

“**Gamma**” means the Gamma Entity providing the relevant service. “**Gamma Entity**” means Gamma Telecom Limited, Gamma Network Solutions Limited or Gamma Business Communications Limited.

All Gamma Entities can be contacted at:

Kings House  
Kings Road West  
Newbury RG14 5BY  
Tel: 0333 014 0000  
Email: [DPO@gamma.co.uk](mailto:DPO@gamma.co.uk)

### **Gamma Data Processing Policies**

The processing of the Product Related Personal Data is subject to the following Gamma policies:

- Data Retention Policy
- Data Breach Policy
- Data Subject Request Process
- Data Controller Request Process
- Information Security Policy

Note that Gamma does not use Product Related Personal Data for automated decision taking (including profiling).

### **General Description of Technical and Organisational Security Measures**

The processing by Gamma of Product Related Personal Data is subject to the following technical and organisational security measures:

#### **Design Assessment**

A key factor is the continuous identification and assessment of risk and taking appropriate action to mitigate against said risk. Gamma does this through a governance structure as set out below:

- Architecture Working Group – Chaired by the Design Authority, this working group reviews and approves all new developments and upgrade programmes.
- Quality Steering Group – Chaired by the CEO, a monthly review of overall service performance and service improvement plans.
- Capacity Planning Forum Chaired by the Operations Director – monthly session whereby the utilisation of every network component is reviewed against planning rules and the sales forecast.
- Change Control Board – Weekly meeting to review every planned change to ensure best practice is followed. Gamma has a comprehensive change control governance structure designed to ensure that planned work does not precipitate significant network problems or introduce additional risk. Regression plans are created for all significant network changes, so that network operations can be resumed in the event of any problems.
- Security and Risk Management meeting – Monthly forum that continuously looks ahead at potential risks and threats to Gamma services and takes action to mitigate / remove as deemed necessary.

- Internal Service reviews – Monthly forums that focus on each individual platforms, these feed into the sessions above as appropriate, this includes reviewing known issues, trends in reported issues, corrective actions, risk log review, any incidents and associated follow up actions, security risks, resourcing and training requirements, supplier review and any product updates.

Gamma operates its own Network Operations Centre (NOC) 24x7x365. This is manned, on premise, by a minimum of two qualified Engineers at any one point in time. The NOC is collocated with our technical support and core engineering teams. Gamma has a standby location should the prime NOC facility become unusable for any reason.

### Testing

Gamma follows different testing mechanisms to ensure the measures Gamma has in place will work effectively when they are called upon, in summary these include:

- Gamma follows all the vendor recommended maintenance procedures for our platforms. Some of these procedures including routine failovers to exercise the HA (High Availability) functionality deployed in certain parts of the architecture.
- Gamma change control process requires failover scenarios to be tested before being placed in the live environment.
- As with any other operator Gamma will see failures of individual components occur on a reasonably frequent basis. Any failure is reviewed to ensure the system reacted correctly and any anomalies are followed up with the respective Engineering teams (internal and external as appropriate).
- The ability to operate from multiple locations is tested on a daily basis. Gamma technical teams regularly work from different locations.
- Gamma tests its ancillary services such as battery backup and generators to a regular schedule.

Individual engineers are allocated lab time to practice component failure and system rebuilds. This allows them to keep their knowledge fresh as well as testing out the procedures.

### Security Certifications

Gamma Telecom is ND1643, ISO27001, Cyber Essentials and ISO22301 certified.

### Product Related Personal Data Processing Information

The services under which Gamma processes Product Related Personal Data and the details of such processing are:

1. [Horizon – Order Management](#)
2. [Horizon – Service Management](#)
3. [Horizon – Corporate Directory](#)
4. [Horizon – Call Recording](#)
5. [Horizon – Next Generation Call Recording - MiFID II call recording option](#)
6. [SIP Trunking – Emergency Calls](#)
7. [SIP Trunking – Call Manager](#)
8. [Inbound Portal](#)
9. [Mobile – ManageMyMobiles](#)
10. [Card Payment Service – Semafone](#)
11. [Contact Centre Service – Serenova](#)
12. [Contact Centre Service – Cirrus](#)

For the purposes of the tables below any reference to:

“**Reseller**” shall mean a company that purchases services from Gamma for the purpose of reselling them to its end customers; and

“**Customer**” shall mean a customer who purchases services directly from Gamma for its own consumption.

## Horizon – Order Management

Description	Details
Subject matter of the processing	Administration and Site contacts processed on the Gamma Portal
Duration of the processing	Duration of the service
Nature and purposes of the processing	Reseller provisions end customer roles needed to create a new Horizon company on the sub-section of the Gamma Portal allocated to the Reseller with the minimal amount of end customer configuration. For direct Customers, Gamma creates Customer roles needed to manage the Horizon service. The process provides portal access for the Customer Administrator to tailor the Horizon service to their needs.
Type of Personal Data	<p><u>Customer Administrator</u> contact details (first name, last name, admin email address, support email address, phone number, mobile number, default domain) used to send a Welcome invitation email and initial login details.</p> <p><u>Customer Main Site contact</u> details (name, email, site address, sub premises, site postcode, phone number, mobile number) which is a mandatory requirement for a new Horizon service</p> <p><u>Fraud Management contact</u> (email addresses, mobile number) used by Partners to register where fraud alert emails are to be sent</p>
Categories of Data Subject	Employees or representatives of Reseller and Customer
Data Retention Period:	Data is retained for the duration of the contract
Sub-processors:	None
Transfers outside the EEA:	None

Version 0.3 – December 2019

## Horizon - Service Management

Description	Details
Subject matter of the processing	Administration managed through the Horizon Company portal
Duration of the processing	Duration of the service
Nature and purposes of the processing	<p>Horizon Administrators can be created and removed from an end customer. Administrators are granted permission to perform a number of service tasks, such as adding, managing and deleting end users on the hosted telephony service.</p> <p>All end users will be deleted in order to cease the Horizon end customer. Each end user can then be assigned telephone numbers, call policies and other voice related services as required. Users may be allocated a voicemail direct dial number to access voicemails when not connected to Horizon devices. User summary call statistics can be viewed on the Horizon portal for inbound and outbound calls</p>
Type of Personal Data	<p><u>Administrator</u> details (Username, First and Last names, email address, Administrator type)</p> <p><u>End user details</u> (Title, first name, last name, DDI phone number, extension, email address, site name, unique end user name/domain, display first and last names, business mobile number)</p> <p><u>Voicemail Identifier</u> (personal voicemail DDI assigned to the User)</p> <p><u>User Call Statistics</u> (calling number, destination number, call outcome) for a summary calls made by a User</p>
Categories of Data Subject	End user and Administrator contacts details
Data retention period:	<p>End user contact data is deleted at the point that the end user is ceased and removed from the Horizon service</p> <p>Administrator details and associated access permissions can be deleted, as required.</p>
Sub-processors:	None
Transfers outside the EEA:	None

Version 0.3 – December 2019

## Horizon – Corporate Directory

Description	Details
Subject matter of the processing	Provision of the corporate phone directly feature in the Horizon hosted platform. Horizon users can be created, edited and deleted by an Administrator based on their own needs and associated to a site.
Duration of the processing	Term of the contract with the customer for this service
Nature and purposes of the processing	<p>Collection, organisation and listing of Customer or end customer employees and their telephone numbers listed and available through the Horizon telephone handset displays to the customer and its employees.</p> <p>Corporate Directory can be viewed through Horizon desk phones, soft-clients and Horizon portals. An end user that belongs to a company can only view other end users within that company</p>
Type of Personal Data	<p><u>Horizon User</u>: First name, last name phone number, extension number, email address, site name, username, contact mobile and, where available, call detail records (CDRs)</p> <p><u>Work Address</u>: street, city, county, postcode (optional)</p>
Categories of Data Subject	<ul style="list-style-type: none"> <li>- End users (staff) and third party contact individuals of the Customer; or</li> <li>- End users (staff) and third party contact individuals of the end customer of a Reseller</li> </ul>
Data retention period:	<p>Administrator can delete end users</p> <p>All relevant data is deleted by Gamma at the end of the term the service was contracted for</p>
Sub-processors:	None
Transfers outside the EEA:	None

Version 0.3 – December 2019

## Horizon – Call Recording

Description	Details
Subject matter of the processing	Provision of call recording feature in the Horizon telephone platform
Duration of the processing	Resellers' end customers and Customers can set the retention period as required (usually 3, 6 or 12 months).
Nature and purposes of the processing	Recording of calls made to and/or by employees which will be available to the Reseller's end Customer or the Customer and its nominated employees, via the Horizon portal.
Type of Personal Data	Call recordings against a named end user who has setup call recording. Administrators will set permissions as to which 3 <sup>rd</sup> Party Support can access call recordings.
Categories of Data Subject	- Staff of the Customer; or - Staff of the end customer of a Reseller
Data retention period:	The Reseller's end customer or the Customer has 7 days to retrieve a copy of the call recordings at the end of the relevant retention period; after that call recordings are deleted by Gamma
Sub-processors:	None
Transfers outside the EEA:	None

Version 0.4 – December 2019

### **Horizon – Next Generation Call Recording**

MiFID II call recording option

Description	Details
Subject matter of the processing	Provision of call recording feature in the Horizon telephone platform
Duration of the processing	Retention period selected by the Reseller's end customer or the Customer (usually 3, 6 or 12 months)
Nature and purposes of the processing	Recording of calls made to and/or by employees which will be available to the end customer and its nominated employees
Type of Personal Data	Call recordings against a named end user who has setup call recording. Administrators will set permissions as to which 3 <sup>rd</sup> Party Support can access call recordings.
Categories of Data Subject	<ul style="list-style-type: none"> <li>- Staff of the Customer; or</li> <li>- Staff of the end customer of a Reseller</li> </ul> <p>Receive a welcome email to login to the next generation call recording platform.</p>
Data retention period:	The end customer of the Reseller or the Customer has 7 days to retrieve a copy of the call recordings at the end of the relevant retention period; after that call recordings are deleted
Sub-processors:	Aeriandi Limited
Transfers outside the EEA:	None

Version 0.3 – December 2019

**SIP Trunking – Emergency Calls**  
(for Resellers only)

Description	Details
Subject matter of the processing	End customer contact details related to emergency call
Duration of the processing	For the duration of an active SIP endpoint
Nature and purposes of the processing	End customer site contact details used when activating numbers on a SIP Trunk for the purposes of managing emergency calls. The contact details are provided to the UK emergency services central handling agency, handled by BT plc.
Type of Personal Data	<p><u>Endpoint site contact</u> details (company, address, postcode) used to identify the premises</p> <p><u>End customer</u> contact details (title, first name, last name, email address, phone number) used as further on site contact information</p>
Categories of Data Subject	Employees of the end customer
Data retention period:	Data is retained until the SIP endpoint is ceased, or the phone number is exported or de-provisioned
Sub-processors:	BT plc
Transfers outside the EEA:	None

Version 0.6 – December 2019



## SIP Trunking – Call Manager

Description	Details
Subject matter of the processing	SIP Trunk Call Manager provisioned on the Gamma Portal
Duration of the processing	Duration of the service
Nature and purposes of the processing	Resellers or Customers create a new Administrator logon which allows the Reseller's end customer or the Customer to manage their call plans and to record event logs associated to their endpoints.  End user contacts
Type of Personal Data	<u>Administrator</u> details (first name, last name, username and email address) used to create a STCM portal logon to allow the Reseller's end customer or Customer to self-manage their calling and disaster recovery plans, and view their service. End customers or Customers can reset logons, add, delete and modify administrators  <u>Notification contact details</u> (email address, username, first name, last name) provided by end user to be automatically notified of important service events, such as call plan updates, chargeable add-on notifications, missed call notifications, new voicemail and voice-to-email notification emails. The end user can opt-in by providing a valid email address for each particular purpose.  <u>Reporting contact</u> (email address) provided by end user to receive advance call management reports for their endpoint, if they have opted into this service
Categories of Data Subject	Employees or representative of Reseller's end customers and Customers
Data retention plan:	Data is retained until the endpoint is ceased
Sub-processors:	None
Transfers outside the EEA:	None

Version 0.3 – December 2019

**Inbound Portal**

Description	Details
Subject matter of the processing	Inbound call management provisioned on the Gamma Portal
Duration of the processing	Duration of the service
Nature and purposes of the processing	<p>Resellers or Customers create a new Administrator logon which allows the Reseller's end customer or the Customer to manage their call plans and to record event logs associated to their endpoints.</p> <p>End user contacts</p>
Type of Personal Data	<p><u>Administrator</u> details (first name, last name, username and email address) used to create a STCM portal logon to allow the Reseller's end customer or Customer to self-manage their calling and disaster recovery plans, and view their service. End customers or Customers can reset logons, add, delete and modify administrators</p> <p><u>Notification contact details</u> (email address, username, first name, last name) provided by end user to be automatically notified of important service events, such as call plan updates, chargeable add-on notifications, missed call notifications, new voicemail and voice-to-email notification emails. The end user can opt-in by providing a valid email address for each particular purpose.</p> <p><u>Reporting contact</u> (email address) provided by end user to receive advance call management reports for their endpoint, if they have opted into this service</p>
Categories of Data Subject	Employees or representative of Reseller's end customers and Customers
Data retention plan:	Data is retained until the endpoint is ceased
Sub-processors:	None
Transfers outside the EEA:	None

Version 0.1 – December 2019

## Mobile – ManageMyMobiles

Description	Details
Subject matter of the processing	Management of mobile services allocated to personnel
Duration of the processing	Duration of the service
Nature and purposes of the processing	<p>Resellers or Customers create new Administrator logons which allows the Reseller' end customer or the Customer to manage all mobile numbers within their named Company. Administrators can assign names (labels) to their mobile services, as well as opt-in to receive global usage alerts and perform a limited number of network service configuration updates.</p> <p>Subscribers (mobile service end users labels) are created as part of a company and may be assigned to a named group.</p>
Type of Personal Data	<p><u>End customer or Customer contact details</u> (name, email, phone number, reseller reference, address, postcode)</p> <p><u>End customer or Customer Administrator contact details</u> (name, role, email address)</p> <p><u>Mobile Subscribers [end users]</u> (first name, last name, email address, mobile number, group, and, where available, call detail records (CDRs))</p>
Categories of Data Subject	Employees or representatives of Customer and/or end customer or a Reseller
Data Retention Period:	All data is removed when the Mobile Company is deleted, or the Manage My Mobile service ceases
Sub-processors:	None
Transfers outside the EEA:	None

Version 0.3 – December 2019

## Card Payment Service – Semafone

Description	Details
Subject matter of the processing	Provision of the Semafone card payment security service to customers
Duration of the processing	The below personal data will be processed in connection with providing and maintaining software for the duration of the contract with the customer, such shorter period where the processing is no longer authorised and in respect of any post-termination processing activities permitted by the customer from time to time
Nature and purposes of the processing	<p>The personal data will be subject to the following basic Processing activities in relation to the types of personal data, described below:</p> <ul style="list-style-type: none"> <li>• Providing and maintaining software to allow individual customers of the customer and/or customer's affiliate to enter payment card details via their telephone keypad and mask the Dual Tone Multi Frequency tones, in accordance with PCI DSS</li> <li>• Personal Data is required by the customer's Payment Service Provider as required for the payment authorisation process</li> </ul>
Type of Personal Data	<ul style="list-style-type: none"> <li>• Name</li> <li>• Postal address</li> <li>• Email address</li> <li>• Phone number</li> <li>• Bank account details</li> <li>• Name on card</li> <li>• Date of birth</li> <li>• Credit or debit card number</li> <li>• Transaction details</li> <li>• CVV</li> <li>• Expiry date</li> </ul>
Categories of Data Subject	Individual customers of the customer and/or customer's affiliate
Data retention period:	The below personal data will be processed in connection with providing and maintaining software for the duration of the contract with the customer, such shorter period where the processing is no longer authorised and in respect of any post-termination processing activities permitted by the customer from time to time
Sub-processors:	Semafone Limited (provider of the service)
Transfers outside the EEA:	None

Version 0.1 – September 2018

### Contact Centre Service – Serenova

Description	Details
Subject matter of the processing:	Provision of the contact centre services by Serenova
Duration of the processing:	Lifetime of the contract, although call recordings are archived after 12 months and reporting metadata after 3 years
Nature and purposes of the processing:	<p>The Personal Data processed will be subject to the following basic processing activities:</p> <p>Serenova, acting as a processor, will, depending on the scope of its engagement, process the personal data to perform the Services, to comply with its statutory and regulatory obligations, to maintain accounts and records. This will involve, among other things, the collection, storage, analysis and disclosure of personal data that Serenova receives from (or on behalf of) the Customer in accordance with the Agreement</p>
Type of Personal Data:	Audio calls and associated recordings and metadata, webchat transcripts, emails
Categories of Data Subject:	<p>The personal data processed may concern the following categories of data subjects:</p> <p>Data subjects may include Customer's employees, contractors, customers or customer end users and employees, as may be further specified in the Agreement</p>
Data retention period:	Lifetime of the contract, although call recordings are archived after 12 months and reporting metadata after 3 years
Sub-processors:	Serenova LLC
Transfers outside the EEA:	None

Version 0.1 – July 2019

## Contact Centre Service – Cirrus

Description	Details
Subject matter of the processing:	Provision of the contact centre services provided by Cirrus
Duration of the processing:	<ol style="list-style-type: none"> <li>1. Call recordings – 7 days</li> <li>2. Call Logs – Calling Line Identification (CLI): 7 years; detailed call log information: 65 days</li> <li>3. Collected Data Variables – as selected by the customer (end of call, 65 days, more than 65 days)</li> <li>4. Data subjects’ information – as selected by the customer</li> </ol>
Nature and purposes of the processing:	The provision of the contact centre services requires Cirrus to process personal data of the individuals using the services, given the customer the ability to determine in most cases which data is processed and how long it is retained
Type of Personal Data:	<ol style="list-style-type: none"> <li>1. Call recordings</li> <li>2. Call Logs</li> <li>3. Collected Data Variables</li> <li>4. Data subjects’ information including: <ul style="list-style-type: none"> <li>– Name</li> <li>– Address</li> <li>– Telephone number(s)</li> <li>– Email addresses</li> <li>– IP address</li> <li>– Date of birth</li> <li>– Twitter username</li> <li>– Facebook username</li> <li>– Facebook home town</li> <li>– G-Suite username</li> <li>– Gender</li> <li>– Apple ID username</li> <li>– Data subject’s image (from social media profile pictures)</li> <li>– Location data</li> <li>– Contact lists (customers, customer locations, suppliers)</li> </ul> </li> </ol>
Categories of Data Subject:	Employees, suppliers and customers of the Customer to whom the contact centre services is provided, and any other relevant third party contacts of the customer
Data retention period:	Data is deleted at the end of processing (see above)
Sub-processors:	Cirrus Response Limited (provider of the service)
Transfers outside the EEA:	None

Version 0.2 – December 2019