Service and support commitments with further insight and details including certifications and Data management

|  |  |
| --- | --- |
| ***Supplier name*** | Quant-CX Ltd |
| ***Address*** | Unit 1a Sole End Business ParkAstley Lane, BedworthNuneatonCV12 0NE |
| ***Contact name*** | Pete Tierney |
| ***Contact email*** | pete@quantrax.co.uk |
|   |
| ***Contact telephone*** | 07948800069 |

Contents

* **Software Services**
* **Supplier self-certification statements with service and support commitments**
* **Please insert supplier details below**
* **Introduction**
* **Supplier commitments**
* **Using the Supplier**
* **Supplier Response - Overarching Legal Requirements**
* **Supplier Response - Data Processing Obligations**
* **Supplier Response - Data Confidentiality**
* **Supplier Response - Data Integrity**
* **Supplier Response - Service Availability**
* **Supplier Response - Transfers beyond the European Economic Area (EEA)**
* **Supplier Response - Use of Advertising**

When entering into an agreement with a service provider that includes, “cloud” services, every controller has to be satisfied that the relevant service provider is carrying out its data processing as per their requirements (ensuring compliance with GDPR by the data controller and also the data processor by default).

It is the responsibility therefore to ensure compliance with the GDPR. This document is meant to act as an aid to that decision-making process by presenting some key questions and answers that should be sought from any potential cloud service provider.

The principles of GDPR are summarised by the Information
Commissioner’s Office

**Supplier Commitments**

In order that the customer can be confident regarding the accuracy of the self-certification statements made in respect of the Quant-CX cloud service, the supplier confirms:

* that their self-certification responses have been fully and accurately completed by a person or persons who are competent in the relevant fields
* that their self-certification responses have been independently verified for completeness and accuracy
* that they will update their self-certification responses promptly when changes to the service or its terms and conditions would result in their existing compliance statement no longer being accurate or complete
* that they will provide any additional information or clarification sought as part of the self-certification process
* that if at any time, the Department is of the view that any element or elements of the service provider’s self-certification responses require independent verification, they will agree to that independent verification, supply all necessary clarification requested, meet the associated verification costs, or withdraw their self-certification submission.

**Beyond the Supplier Services**

When reviewing supplier, you may wish to consider aspects of data security beyond the supplier-highlighted. These could include:

* how your organisation chooses to use the provided service
* the nature, types and sensitivity of data your organisation chooses to place in any accessible cloud service
* the extent to which your organisation adapts its own policies (such as acceptable use, homeworking, Bring Your Own Device (BYOD) and staff training to ensure that the way staff and students use the service is consistent with UK DPA guidance and GDPR. Please refer to the Information Commissioner’s Office (ICO) BYOD guidance
* the wider policies and practices your organisation has in place to ensure that the use of Quant-cx Ltd Services by their staff and students remains DPA and GDPR compliant,
* the use of robust, strong, frequently changed authentication passwords and encryption keys, policies on BYOD / homeworking / acceptable use

**Q&A- Overarching Legal Requirements**

 your organisation are required to ensure that all Quant-cx Ltd Services used enable them to meet their legal obligations under the DPA and GDPR. To assist your organisation in that assessment, Quant-CX Ltd provides full documentation on details of this at agreement sign off

|  |  |  |
| --- | --- | --- |
| Question | Suppli er Resp onse Code | Response Statement with Supporting Evidence (where applicable) |
| Q 1 – Does your standard contract for the supply of Quant-cx Ltd Services to UK fully comply with the DPA and GDPR? |   | Yes – our contract states the QuantCX service will be delivered in accordance with local Data Protection Act 1998 and current GDPR legislation ( last updated June 2020) |
| Q 2 – If your standard contract does not fully comply with the DPA, do you offer additional commitments to help ensure such compliance? |   | N/A Quant-CX Ltd is fully compliant |
| Q 3 – Is your contract with UK customers enforceable both in the UK and in the country in which your company is registered? |   | Yes - Quant-CX is a UK registeredcompany and contracts are enforceable under UK law. |
| Q 4 – Do your services ensure that your organisation are able to comply with theirobligations with regard tothe exercise of data subjects’ rights?.  |  | Yes- Your organisation has full control |

**Supplier Response - Data Processing Obligations**

GDPR and The Data Protection Act (DPA) and wider relates to personal data that is processed and is likely to be relevant to most of the operations that comprise a cloud computing service. This includes simple storage of data, the obtaining and handling of information, operations such as adaptation, organisation, retrieval and disclosure of data, through to erasure or destruction.

your organisation, as data controllers, have a responsibility to ensure that the processing of all personal data complies with GDPR and the DPA and this includes any processing carried out on their behalf by a cloud service provider.

To assist your organisation in understanding whether the cloud service being provided by Quant-CX Ltd is likely to comply with GDPR and the DPA in relation to data processing, Quant-CX Ltd has responded as follows

|  |  |  |
| --- | --- | --- |
| Question |  | Response Statement with Supporting Evidence (where applicable) |

|  |  |  |
| --- | --- | --- |
| Q 1 – Taking account of the UK Information Commissioner's Office (ICO) guidance on Data Controllers and Data Processors, when providing the service, do you act at any time as a data controller in respect of the data processed as part of this service? |   | No – Your organisation will be data controllers. |
| Q.2 – Where you act as a data processor does your contract ensure that you will only act on the instructions of the data controller? |   | Yes – Quant-CX will only act oninstructions given by an authorisedcontact within Your organisation and process data in accordance with the DPA 1998 and fully compliant under GDPR |
| Q. 3 – Does your contract document the security measures that you implement to enable Your organisation to ensure compliance with the DPA's security obligations? |   | Yes – the Quant-CX Data ProtectionPolicy and Privacy Policy  |
| detail the security measures Quant-CX employs to ensure compliance with GDPR and the DPA’s security obligations and can be found on our website. |
| Q 4 – Is the processing of personal data or metadata limited to that necessary to deliver [or improve] the service? |   | Yes – customer data and meta data is only used to deliver the service. |
| Q 5 – Where your contract does not cover every aspect of data processing, are you prepared to enter into a separate data-processing agreement with your Quant-cx Ltd Cloud Services |  | N/A The Quant-CX contract covers every aspect of data processing. |

**Supplier Response Data Confidentiality**

When choosing a service provider, Your organisation must select a data processor providing sufficient guarantees about the technical and organisational security measures governing the processing to be carried out, and must take reasonable steps to ensure compliance with those measures.

The cloud customer should therefore review the guarantees of confidentiality that the cloud provider can commit to. To assist in understanding if the service being provided by Quant-CX Ltd is likely to comply with UK law in relation to data confidentiality Quant-CX Ltd has responded as follows:

|  |  |  |
| --- | --- | --- |
| Question | Suppli er Respo nse Code | Response Statement with Supporting Evidence (where applicable) |
| Q 1 – Do you prohibit personal data or metadata being shared across other services that you as a supplier do or may offer? |   | Yes – Quant-CX only provides the Quant-CX Mass Notification, Response and Location service - no data is shared with other services, suppliers or any external organisation. |
| Q 2 – Do you prohibit personal data or metadata being shared with third parties? |   | Yes – no data or meta data is shared with third parties. |
| Q .3 – Does your service have a robust authentication process in place to protect access to personal data and/or user accounts? |  | Yes – administrative access to the Quant-CX Management Portal is via https and is protected using two-factor authentication. End users have to be authenticated against their registered details.Data at rest is stored using a 256 AES encryption. |
| Q 4 – Does your servicehave in place arrangementsto assist Your organisation inprotecting access topersonal data and/or useraccounts? |  | Yes – administrative access to the Quant-CX Management Portal is via https and is protected using two-factor authentication. End usershave to be authenticated against their registered details these details are stored using a 256 AES encryption. |
| Q.5 – Are appropriatecontrols in place to ensureonly authorised staff haveaccess to client/customer data? |  | Yes – access is restricted to Quant-CXstaff who are registered on theservice and have the correct login/authentication details. |

The following questions address the supplier approach to data encryption. The ICO guidance on encryption is as follows:

There have been a number of reports recently of laptop computers, containing personal information which have been stolen from vehicles, dwellings or left in inappropriate places without being protected

adequately. The Information Commissioner has formed the view that in future, where such losses occur and where encryption software has not been used to protect the data, regulatory action may be pursued.

The ICO recommends that portable and mobile devices, including magnetic media, used to store and transmit personal information, the loss of which could cause damage or distress to individuals, should be protected using approved encryption software which is designed to guard against the compromise of information.

Personal information which is stored, transmitted or processed in information, communication and technical infrastructures, should also be managed and protected in accordance with the organization’s security policy and using best practice methodologies such as using the International Standard 27001. Further information can be found at https:// www.getsafeonline.org/

There are a number of different commercial options available to protect stored information on mobile and static devices and in

|  |  |  |
| --- | --- | --- |
| Q 6 – Does your cloud service insist that communications with access devices are encrypted? |  | Yes – communication with access devices uses SSL. |
| Does your cloud service ensure that data at rest is encrypted? |  | Yes – data at rest uses a 256 AES encryption. |
| Does your cloud service ensure that data in transit between your data centres is encrypted? |  | Yes – data in transit is encrypted with SSL. |
| Does your service ensure that email traffic between your cloud service and other cloud service providers can be encrypted? |  | Yes – the only email transmission between the Quant-CX cloud service and the end user is a welcome email sent to Administrators ,to enable them to login and set a password. This is transmitted using secure SMTP. |
| Does your service provide defined timescales in respect of data destruction and deletion both during the contract and at contract end? |  | No – deleting end user details is inthe control of the end customer. Removing deleted messages storedin the Quant-CX cloud service is undertaken manually by Quant-CX at the request of the end customer. |
| Does your service ensure that you use a secure deletion and erasure process which encompasses all copies of client/customer data? |  | Yes – Quant-CX uses a secure deletion and erasure process, should this be required. |

**Data Integrity**

Data integrity has been defined as “the property that data is authentic and has not been maliciously or accidentally altered during processing, storage or transmission”. To assist Your organisation in understanding if the cloud service being provided by Quant-CX Ltd is likely to comply with the DPA in relation to data integrity Quant-CX Ltd has confirmed the position to be as follows:

|  |  |  |
| --- | --- | --- |
| Do you allow a trusted independent third party to conduct regular detailed security audits of the physical, technical and organisational aspects of your service? |  | Yes – Quant-CX employ PIN services Ltd to perform this service. |
| Where the above audits are conducted, do you make the findings available to current and/or prospective cloud customers? |  | Yes – Quant-CX will make thisinformation available on request tocurrent and prospective cloud customers. |
| Does your service ensure that where such audits are carried out, they are conducted to best industry standards? |  | Yes – all tests are carried out to industry standard by PIN services who are a market leader in this is area. |
| Are audit trails in place enabling users to monitor who is accessing their data? |  | No – audit trials are not currently available but access is restricted to only the authorised administrators of the service who are nominated by the customer. |
| Does your service ensure you could restore all |  | Yes – the Your organisation is also provided |
| customer data (without |  | with the facility to restore end user |
| alteration) from a back-up if you suffered any data loss? |  | contact data. |

**Service Availability**

Service availability means ensuring timely and reliable access to personal data. One threat to availability in the cloud which is often outside the responsibility of the cloud service provider is the accidental loss of network connectivity between the client and the provider of service.

Data controllers should therefore check whether the cloud provider has adopted reasonable measures to cope with the risk of disruptions, such as backup internet network links, redundant storage and effective data backup mechanisms.

To assist Your organisation in understanding if the service being provided by a particular company is likely to comply with the DPA in relation to service

Availability has confirmed as follows

|  |  |  |
| --- | --- | --- |
| Can you confirm that you have sufficient capacity to ensure you can provide a resilient, reliable and accessible service at all times? |  | Yes – Quant-CX is constantlymonitoring it’s cloud service and measuring customer requirements to ensure sufficient capacity is always available to deliver a highly resilient, reliable and accessible service. |
| Does your service offer guaranteed service levels? |  | Yes – Quant-CX can provide details of it Service Level Agreement on request to current and prospective customers. |
|  Does your service provide remedies to customers in the event that service levels are not met? |  | Quant-CX always achieves its service levels. However, our service team would be available to help remedy problems and provide advice on the service, should this ever not be the case. |

The key areas that cloud service providers are invited to respond against in respect of a serious incident are:

· Solution configuration

· Communicating serious breaches

· Supplier responsibilities

· Restoring data

· Managing media attention

· Engaging with the child protection agencies

· Engaging with the wider Your organisation community

These are minimum suggested areas and suppliers are free to set out additional support capabilities which could be used in the event of a serious incident and which they feel will engender confidence in Your organisation and differentiate the supplier in this competitive and growing marketplace.

**ADDRESSING SERIOUS INCIDENTS**

Cloud service providers should as a minimum clarify in this area of their response:

· How Your organisation should log any serious issues regarding the use of the service, providing as a minimum a UK phone number and support email address. It is better to provide an indication of the individuals or roles that should be the first point of contact – for example “you should also contact our Head of Security

·The nature of the support that might be available – for example, is it limited to phone and/or email or are there circumstances when on-site support might be required.

· How the cloud service provider might work with Your organisation to address the consequences of the serious incident

· Whether in addition to contacting the incident support centre there are other resources that could be made available – for example via online tools and resources, a partner ecosystem, a local public sector or education support team or identified escalation routes within the company that should be utilised.

Supplier response:

If a serious incident should occur Your organisation should follow the standard service support procedure as detailed in their Quant-CX Customer Service Plan

**SUPPLIER RESPONSIBILITIES**

In this section cloud service providers should, as a minimum, set out (in language aimed at Your organisation managers), their responsibilities when working with Your organisation to address the implications of a serious incident.

In addition, cloud service providers should describe what practical assistance they would be able to offer which goes beyond the “contractual minimum” as set out in their terms and conditions.

Supplier response:

It is Quant-CX’s responsibility, as detailed in our Customer Service Plan, to support the availability of the service, the resilience of the Quant-CX cloud, ensure the security of the Quant-CX service (and the associated customer data) and to respond to customer issues.

Quant-CX would prioritise the recovery from of a serious incident and would work with Your organisation management team to ensure the incident is resolved in a timely manner. Additionally Quant-CX would put measures in place to prevent such an incident reoccurring and provide a full incident report for auditing purposes.

If required Quant-CX would engage with Your organisation third party suppliers and consultants for further planning and reporting purposes.

SOLUTION CONFIGURATION.

Whilst virtually all cloud service providers have detailed technical advice on how their systems should be configured, this section of the supplier response should set out the general principles which Your organisation management should expect to see implemented to ensure maximum security of their cloud implementation.

This might cover for example:

· The need for correct configuration of access devices

· The use of additional backup / data synchronisation arrangements for sensitive or business critical data

· Configuration options or additional services that provide greater level of security than is available in your free offering

· Sample password policies in relation to the age and ability of the users of their service

· Policies in respect of helpdesk and security staff access to client data

Supplier response:

In order to deliver the Quant-CX service Your organisation must provide their main points of contact for technical/service support. These contact will have the ability to request password changes via an authenticated process and changes to the service configuration.

Your organisation must also provide contact details for those individuals, within Your organisation, who will have administrative access to the Quant-CX service. These administrators will have the ability to send messages, view message responses, view end user locations and input/manage end user data. They will be provided with an ID and Password to access the Quant-CX Management Portal and they are advised they should also enable Quant-CX’s two factor authentication to further secure access to their service.

End users within private groups will have to authenticate themselves against their contact data registered on the service and will also have to enter a code, sent to their mobile device to gain access to the Quant-CX app message group(s). At present it is optional for end users to share their location but this can be stimulated by the delivery of a message requesting the end user shares their location details. Alternatively this function can be controlled via an Enterprise Mobile Management service - Quant-CX integration work may be required with such a capability.

RESTORING DATA

Where a serious event had occurred which resulted in the loss of data by Your organisation, cloud service, providers should set out what steps they would take to work with Your organisation to recover and restore to the maximum extent possible the data which has been lost (or corrupted). This section should also include indicative timescales.

Supplier response:

Quant-CX provides a highly secure service with a mirrored architecture delivered from geographically disperse ISO 27001 data centres - these are in three separate locations in the EU.

The Quant-CX geo-redundant architecture is designed to provide real time back-up of data and automatic recovery if a node should fail. If, however, an eventuality occurred that resulted in data loss, the customer is equipped to restore their contact data to the Quant-CX service – this will enable continuity of service. It would be Quant-CX’s responsibility to recover and restore lost message data, which it would do in line with it’s Customer Service Plan i.e. service restoration within 4 hours for a loss of service incident affecting all users.

MANAGING MEDIA ATTENTION

Where a serious event had occurred which resulted in significant media attention falling on Your organisation, suppliers should indicate the steps they would take as a responsible service provider to work with Your organisation in managing the media attention.

Supplier response:

Quant-CX would be guided by Your organisation and adhere to their media management policy and process.

In the event of a serious incident that may have implications on the Your organisation staff, pupils, parents, as well as the wider community, it is Quant-CX’s policy not to engage directly with the media unless they are directed to do so by Your organisation. Quant-CX will support Your organisation response to the media, working in collaboration with Your organisation and any relevant stakeholders.

ENGAGING WITH CHILD SUPPORT AGENCIES

Where a serious event had resulted in issues being raised that related to child protection – for example the loss of sensitive pupil data, the cloud service provider should indicate what it would do to assist the Your organisation in engaging with the relevant child protection agencies, over and above the contractual minimum.

Supplier response:

The Quant-CX service has been designed to provide a highly secure service that safeguards sensitive pupil data. If, however, a serious incident occurred that related to child protection, Quant-CX’s senior management would support the Your organisation and work collaboratively with the Child Protection Agencies. An authorised contact at Your organisation will be supplied with the relevant contact information for a member of the senior management team, which is accessible on a 24x7x365 day year basis.

 Engaging With the Wider Organisation Including Your Community

Where a serious incident had resulted in issues being raised that related to the wider Your organisation community – for example parents, the local authority, the curriculum or examination bodies or the Information Commissioners Office, the cloud service provider should indicate what it would do to assist Your organisation in engaging with the relevant organisation to address the implications of the serious incident. Again, this should describe available support over and above the contractual minimum.

Supplier response:

The Quant-CX service has been designed to provide a highly secure service that safeguards sensitive pupil data. If, however, a serious incident occurred that affected the wider Your organisation community, Quant-CX’s senior management would support Your organisation and work collaboratively with relevant agencies or organisations. An authorised contact at Your organisation will be supplied with senior management contact information, which is accessible on a 24x7x365 basis.

For any other enquires then please direct these through your contact or in writing to us