

GDPR & your Contract with Advanced Computer Software Group Ltd

As an existing customer or partner of Advanced it is important that you read the information below regarding changes to your existing contract with us to accommodate the General Data Protection Regulation (GDPR).

New data protection legislation is due to come into force during May 2018, which aims to protect the privacy of all EU citizens and prevent any data breaches of EU citizen's personal data. It will apply to any public or private organisation processing personal data.

Established key principles of data privacy will remain relevant in the new data protection legislation but there are also a number of changes. Amongst the changes, the new GDPR specifies that any processing of personal data by a Data Processor should be governed by a contract with certain provisions included.

This will involve both your organisation and ours updating our existing contract terms and conditions (Prime Agreement) and ensuring we agree a schedule to clarify the roles and responsibilities between your organisation as the Data Controller and Advanced as the Data Processor.

Enclosed is our proposed 'Data Protection addendum' (which is based on the standard Crown Commercial Services clauses relevant to G-Cloud for ease of review). For the avoidance of doubt, the term 'Customer' within the addendum refers to both customers and partners of Advanced. We kindly request that you forward this communication, along with the enclosed Data Protection Addendum, to an authorised signatory for your company. We request that the signed Data Protection Addendum is returned to us as soon as possible and in any event no later than 30th March 2018. Should you have any queries regarding this, we have a dedicated email address gdpr@oneadvanced.co.uk.

If you do not sign and return the enclosed Data Protection Addendum by 30th March 2018, but continue to work with any of the entities within the Advanced group as per the Prime Agreement we have between us, you will be deemed to have agreed it. Nevertheless, as it is a statutory requirement for both organisations to update their contracts as required and be able to evidence this, we would appreciate you returning a signed copy of the Addendum prior to 30th March 2018 to acknowledge your consent to the new provisions.

We have provided additional resources around GDPR including an FAQ document which answers customer queries about our GDPR obligations, Technical and Organisational measures, Sub-processors and the Data Protection Compliance framework at Advanced. We have also updated the [Support Handbook](#) to reflect changes in the support process.

We thank you for your attention and please contact us on the email address with any queries.

Sincerely,

Advanced Data Protection Office

ADDENDUM TO IMPLEMENT LEGISLATIVE OBLIGATIONS RELATING TO DATA PROCESSING OF PERSONAL DATA AND DATA SUBJECTS

This Addendum is entered into on the date of signature of the last party hereto and is supplemental to all terms and conditions currently in place between the Customer and Advanced but replaces any provisions in such terms and conditions relating to the processing of Personal Data by Advanced.

IT IS HEREBY AGREED AS FOLLOWS:

1. The following definitions will apply:

“Advanced” means the contracting party set out in the Original Agreement, being a company, which is ultimately owned by the Holding Company;

“Applicable Law” means the laws of England and Wales (and any EU regulations from time-to-time applicable (i) whilst the United Kingdom remains a member of the European Union or (ii) subsequently under the terms of the European Union (Withdrawal) Bill);

“Controller” has the meaning set out in the Data Protection Legislation;

“Customer” means the contracting party set out in the signature block at the end of this Addendum;

“Data Loss Event” means any event that results, or may result, in unauthorised access to Personal Data held by Advanced hereunder, and/or actual or potential loss and/or destruction of Personal Data in breach of the Clause DP, including any Personal Data Breach;

“Data Protection Legislation” means all applicable privacy or data protection laws and regulations (as amended, consolidated or re-enacted from time-to-time) which relate to the protection of individuals with regards to the processing of personal data to which a party is subject, including the Data Protection Act 1998 (as may be superseded) and GDPR (on and from 25 May 2018) for as long as any of the above are incorporated into Applicable Law together with any guidance and/or codes of practice issued from time-to-time by the Information Commissioner;

“Data Subject” has the meaning set out in the Data Protection Legislation;

“Data Subject Access Request” means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data;

“EEA” means the European Economic Area;

“GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119/1, 4.5.2016;

“Holding Company” means Advanced Computer Software Group Limited (Co No 05965280) whose registered office is at Ditton Park, Riding Court Road, Datchet, Berkshire, United Kingdom, SL3 9LL;

“Original Agreement” the terms and conditions currently in force between the parties;

“Personal Data” has the meaning set out in the Data Protection Legislation and includes (but is not limited to) special categories of personal data which reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, sex, sexual orientation, trade union membership or the processing of genetic or biometric data, for the purpose of uniquely identifying a natural person;

“Personal Data Breach” has the meaning set out in the Data Protection Legislation;

“Processor” has the meaning set out in the Data Protection Legislation;

“Security Measures” means appropriate technical and organisational measures which are set out in the service description (or other relevant documentation available) for the relevant products or services provided by the Processor;

“Sub-processor” means any third party appointed to process Personal Data on behalf of Advanced related to the Original Agreement.

2. In consideration of the ongoing provision of any services by Advanced after 25th May 2018, the terms of this Addendum will be incorporated into the Original Agreement.
3. Notwithstanding any provisions in the Original Agreement relating to the protection of individuals with regards to the processing of Personal Data, such provisions will be superseded in their entirety and replaced by the following new Clause DP.
4. The following new Clause DP will be inserted into the Original Agreement, as follows:

- “DP.1 The parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and Advanced is the Processor.
- DP.2 Advanced shall notify the Customer immediately if it considers that any of the Customer's instructions infringe the Data Protection Legislation.
- DP.3 Advanced shall provide reasonable assistance to the Customer in relation to compliance with the Data Protection Legislation.
- DP.4 Advanced shall, in relation to any Personal Data processed in connection with its obligations to the Customer:
- DP.4.1 process that Personal Data only in accordance with the Schedule below, unless Advanced is required to do otherwise by Applicable Law. If it is so required, Advanced shall promptly notify the Customer before processing the Personal Data unless prohibited by Applicable Law;
 - DP.4.2 ensure that it has Security Measures in place (available on request) and the Customer hereby confirms that such Security Measures are appropriate to protect against a Data Loss Event having taken into account the:
 - DP.4.2.1 nature of the Personal Data to be protected;
 - DP.4.2.2 harm that might result from a Data Loss Event;
 - DP.4.2.3 state of technological development; and
 - DP.4.2.4 cost of implementing any additional measures;
 - DP.4.3 In relation to the clauses above, the Controller is responsible (as between the parties and to Data Subjects and supervisory authorities) for:
 - DP.4.3.1 ensuring that Data Subjects have given appropriate consent to the processing of any Personal Data by the Processor;
 - DP.4.3.2 ensuring the Security Measures meet the GDPR standard of appropriateness;
 - DP.4.3.3 claims or complaints resulting from Advanced's actions to the extent that such actions directly result from instructions received from the Customer.

In relation to DP.4.3.2, the parties acknowledge that the Processor may not be in a position to assess what measures are appropriate to the Controller's Personal Data (since the data is collected and processed for the purposes of the Controller's and not the Processor's business). The Controller may select chargeable services for additional security measures which exceed the standard security measures provided by the Processor.

- DP.4.4 ensure that:
- DP.4.4.1 Advanced personnel do not process Personal Data except in accordance with this Clause DP (and in particular the Schedule below);
 - DP.4.4.2 it takes all reasonable steps to ensure the reliability and integrity of any Advanced or third party personnel who have access to the Personal Data and ensure that they: (i) are aware of and comply with Advanced's duties under this clause; (ii) are subject to appropriate confidentiality undertakings with Advanced or any Sub-processor; (iii) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Customer or as otherwise permitted hereunder; and (iv) have undergone adequate training in the use, care, protection and handling of Personal Data; and
- DP.4.5 not transfer Personal Data outside of the EEA unless the prior written consent of the Customer has been obtained and the following conditions are fulfilled:


- DP.4.5.1 the Customer or Advanced has provided appropriate safeguards in relation to the transfer (in accordance with GDPR Article 46) as determined by the Customer;
- DP.4.5.2 the Data Subject has enforceable rights and effective legal remedies;
- DP.4.5.3 Advanced complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses all reasonable endeavours to assist the Customer in meeting its obligations); and
- DP.4.5.4 Advanced complies with any reasonable instructions notified to it in advance by the Customer with respect to the processing of the Personal Data;

IT BEING ACCEPTED by the Customer that:

- DP.4.5.5 it is technically possible for hosted systems to be accessed by the Customer from outside the EEA
 - DP.4.5.6 the Customer is responsible for obtaining any necessary consent from Data Subjects in relation to any access by the Customer or licensed third parties to such hosted systems from outside the EEA; and
 - DP.4.5.7 the Customer is liable for any complaints or claims by Data Subjects or third parties resulting from such access.
- DP.4.6 at the written direction of the Customer, delete or return Personal Data (and any copies of it) to the Customer on termination unless Advanced is required by Applicable Law to retain the Personal Data.
- DP.5 Before allowing any Sub-processor to process any Personal Data related hereto Advanced must give the Customer:
- DP.5.1 at least 30 calendar days' notice in writing of the intended Sub-processor and processing;
 - DP.5.2 confirmation that there is a written agreement with the Sub-processor which give effect to the terms set out in this Clause DP such that they apply to the Sub-processor;
 - DP.5.3 such information regarding the Sub-processor as the Customer may subsequently reasonably require.
Advanced shall remain fully liable for all acts or omissions of any Sub-processor.
- DP.6 Advanced currently provides Level 3 support services from outside the EEA through Advanced Business & Healthcare Solutions India Private Ltd, the wholly owned subsidiary, of its Holding Company, which conforms to all necessary requirements and appropriate safeguards under Applicable Law (including GDPR Article 46). No physical transfer of Data takes place during the provision of such support services. Controlled remote access is granted to the staff in India only for the limited purposes of Level 3 support services. Personal Data will be anonymised wherever reasonably practicable to do so in the timeframes available. Compliance with Applicable Law can be provided in writing to the Customer in this regard.
- DP.7 Subject to Clause DP.4, Advanced shall notify the Customer immediately if it:
- DP.7.1 receives a Data Subject Access Request (or purported Data Subject Access Request) relevant to the Customer;
 - DP.7.2 receives a request to rectify, block or erase any Personal Data relevant to the Customer;
 - DP.7.3 receives any other request, complaint or communication relating to either party's obligations under the Data Protection Legislation;
 - DP.7.4 receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data, relevant to the Customer, processed hereunder;
 - DP.7.5 receives a request from any third party relevant to the Customer for disclosure of Personal Data where compliance with such request is required or purported to be required by Applicable Law; or
 - DP.7.6 becomes aware of a Data Loss Event relevant to the Customer.
- DP.8 Advanced's obligation to notify under Clause DP.7 shall include the provision of further information to the Customer in phases, as details become available.

- DP.9 Taking into account the nature of the processing, Advanced shall provide the Customer with full assistance in relation to either party's obligations under Data Protection Legislation and any complaint, communication or request made under Clause DP.7 (within the timescales agreed between the parties) including by promptly providing:
- DP.9.1 the Customer with full details and copies of the complaint, communication or request;
 - DP.9.2 such assistance as is reasonably requested by the Customer to enable the Customer to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
 - DP.9.3 the Customer, at its request, with any Personal Data it holds in relation to a Data Subject;
 - DP.9.4 assistance as requested by the Customer following any Data Loss Event;
 - DP.9.5 assistance as requested by the Customer with respect to any request from the Information Commissioner's Office, or any consultation by the Customer with the Information Commissioner's Office.
- DP.10 Advanced shall maintain complete and accurate records and information to demonstrate its compliance with Article 30 of GDPR.
- DP.11 Advanced shall allow for audits of its security measures and data processing activities by the Customer or the Customer's designated auditor at reasonable times and on reasonable notice.
- DP.12 For the avoidance of doubt, notwithstanding anything to the contrary in the Original Agreement, each party accepts liability for loss of Personal Data to the extent that the loss of Personal Data is caused by:
- a material breach by such party of their data processing obligations under Applicable Law;
 - a failure by such party to provide the Security Measures that it was contractually committed to provide in relation to such Personal Data
- up to the sum of £1,000,000.”
5. Notwithstanding anything to the contrary set out in the Original Agreement, to the extent that there is any duplication or conflict between definitions or clauses used in the Original Agreement and this Addendum, the definitions and clauses set out in this Addendum will apply and take precedence. In all other respects the Original Agreement as amended by this Addendum shall continue in full force and effect.
6. Each party confirms that their signatory set out below is a duly authorised representative and authorised to act on behalf of the relevant party. All the terms of Clause DP are expressly confirmed and consented to by the Customer hereunder.
7. This Addendum is governed by the laws of England and Wales and the parties submit to the exclusive jurisdiction of the courts of England and Wales.

In witness of which the parties have agreed to this Addendum and executed this Addendum by their duly authorised representatives

For and on behalf of Advanced		For and on behalf of the Customer	
Authorised Signatory		Company Name	
		Signature of authorised signatory	
Name	Andrew Hicks	Name	
Position	Chief Financial Officer	Position	
Date	02 March 2018	Date	

Schedule

1. Advanced shall comply with any further written instructions of the Customer with respect to processing by Advanced. Any such further instructions shall be incorporated into this Schedule.

Description	Details
Subject matter of the processing	<p>The services purchased by the Controller, as detailed in the Order Form, including but not limited to:</p> <ol style="list-style-type: none"> 1. Hosting Services 2. Professional Services 3. Software Support Services 4. Software Development 5. IT and Administrative Operations 6. Managed Services / IT Outsourcing Services
Duration of the processing	The term set out for the provision of the relevant software and/or services as stated in the Order Form
Nature and purposes of the processing	<p>Nature of Processing:</p> <ol style="list-style-type: none"> 1. Storage 2. Recording 3. Consultation 4. Remote Access 5. Collection <p>Purposes of processing:</p> <ol style="list-style-type: none"> 1. Hosting – Cloud and platform 2. Software Support services 3. Bespoke software development 4. Project Management 5. Training & Consultancy 6. Payroll services 7. IT services 8. Managed Services / IT Outsourcing Services 9. Migration services 10. Other professional services
Type of Personal Data	This varies from customer to customer, but depending on the products and services purchased may include both personal data and special category data as defined in the GDPR.
Categories of Data Subject	This varies from customer to customer. The Customer will maintain a list of categories of data subjects appropriate to their use of the software or services.
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	Data will be returned to the Customer in a machine readable format on request prior to termination at the cost of the Customer, unless agreed otherwise in the Original Agreement or to the extent it is required to be retained under Applicable Law.



General Data Protection Regulation

Customer & Partner FAQ

Doc Version: 1.0

Advanced | Ditton Park, Riding Court
Road, Datchet, Berkshire, SL3 9LL

t: 0845 160 6162

www.oneadvanced.com

Copyright © Advanced Computer Software Group Ltd 2017

This document contains confidential and / or proprietary information. The content must not be disclosed to third parties without the prior written approval of Advanced Computer Software Group Limited or one of its subsidiaries as appropriate (each referred to as “Advanced”). External recipients may only use the information contained in this document for the purposes of evaluation of the information and entering into discussions with Advanced and for no other purpose.

Whilst Advanced endeavours to ensure that the information in this document is correct and has been prepared in good faith, the information is subject to change and no representation or warranty is given as to the accuracy or completeness of the information. Advanced does not accept any responsibility or liability for errors or omissions or any liability arising out of its use by external recipients or other third parties.

No information set out or referred to in this document shall form the basis of any contract with an external recipient. Any external recipient requiring the provision of software and/or services shall be required to enter into an agreement with Advanced detailing the terms applicable to the supply of such software and/or services and acknowledging that it has not relied on or been induced to enter into such an agreement by any representation or warranty, save as expressly set out in such agreement.

The software (if any) described in this document is supplied under licence and may be used or copied only in accordance with the terms of such a licence. Issue of this document does not entitle an external recipient to access or use the software described or to be granted such a licence.

The development of Advanced software is continuous and the published information may not reflect the current status. Any particular release of the software may not contain all of the facilities described in this document and / or may contain facilities not described in this document.

Advanced Computer Software Group Limited is a company registered in England and Wales with registration number 05965280 whose registered office is at Ditton Park, Riding Court Road, Datchet, Berkshire. SL3 9LL.

A full list of its trading subsidiaries is available at www.oneadvanced.com/legal-privacy

Contents

1. Introduction	4
2. Advanced GDPR Compliance Framework	4
GDPR Requirements	4
Governance and Compliance.....	6
Supplier / Third Party Management	9
Personnel Security	9
Organisation Standards	11
3. Access to Customer Data and/or Network.....	13
Support Services	13
Hosting Services	14
4. Data Processing Outside EEA	17
Support Services	17
Hosting Services	19
5. Technical & Organisational Measures	20
Support Services	20
Hosting Services	22

1. Introduction

This document is prepared by Advanced to answer customer/partner queries around our GDPR obligations, Technical and Organisational measures, Sub-processors and the Data Protection Compliance framework at Advanced.

2. Advanced GDPR Compliance Framework

The Frequently Asked Questions answered in this section are applicable to all the services provided by Advanced, including but not limited to:

- Hosting Services
- Support Services
- Professional Services
- IT and Administrative Operations
- Software Development

2.1 GDPR Requirements	
1.	<p>Q: Is Advanced a Data Controller or a Data Processor when providing services to customers?</p> <p>A: Advanced is the Data Processor with regards to all the services provided to customers and only acts on the documented instructions of the Data Controller (customer).</p>
2.	<p>Q: Who is the Data Owner with respect to customer data?</p> <p>A: The Data Controller is the Data Owner as they control the collection of data and purpose(s) of processing.</p>
3.	<p>Q: Do you have a Data Protection Officer (DPO) and an Information Security Officer (ISO)?</p> <p>A: Advanced has appointed a DPO in compliance with the GDPR requirement. We also have an ISO and our DPO and ISO together form the Data Protection Office and can be reached at dataprotection@oneadvanced.com</p>
4.	<p>Q: What is your stance on GDPR?</p> <p>A: Advanced has a dedicated team of analysts and experts analysing the legislation to understand how we can ensure best practice compliance with the new regulations internally as well as ensuring our products and services are 'GDPR ready'.</p>

5.	<p>Q: What steps are you taking to establish a GDPR compliance framework within your organisation?</p> <p>A: Advanced has been working hard to establish a GDPR Compliance Framework within all parts of the Advanced group. As part of our internal Compliance program, we are updating our policies, processes and procedures as per the GDPR requirements in order to be compliant with GDPR – both as a Data Controller and as a Data Processor. We are also providing training to our staff in order to make them aware of our data protection obligations.</p>
6.	<p>Q: Have you had any data breaches in the last 12 months which you had to report to the Information Commissioners Office (ICO)?</p> <p>A: No.</p>
7.	<p>Q: What type of processing activities will be carried out by Advanced?</p> <p>A: Advanced is responsible for carrying out the processing activities agreed and documented in the contract between Advanced and the Customer. Please refer to the Schedule in the Advanced Data Protection Addendum for details of the processing activities.</p>
8.	<p>Q. How do you ensure the confidentiality and security of the personal data shared with you for carrying out processing activities?</p> <p>A: All data is saved on secure servers within the Advanced (or Advanced managed) infrastructure.</p>
9.	<p>Q: Will your organisation use the data for any other purpose than that specified in the contract?</p> <p>A: No. Advanced will only act on the agreed and documented instructions of the Data Controller.</p>
10.	<p>Q: Will your organisation carry out any sort of marketing activity for the Data Controller?</p> <p>A: No. This is not part of the any of the services provided by Advanced; nor do we use the customer data for our own marketing activities.</p>
11.	<p>Q: What are the categories of the data processed by your organisation?</p> <p>A: Categories:</p> <p>Personal Data: Name, Email, Phone, Job Title, IP address, Bank Details, Employment History, Gender, DOB, Driving Licence, NI no., Passport, Image (Photo), Voice recording, Vehicle registration,</p>

	<p>Sensitive data: health records, criminal convictions, children’s data, political views, Ethnic origin, Sexual orientation, Sex Life, Biometric data, Genetic Data, Religious views, Trade Union membership.</p> <p>The categories vary from client to client. It is the client’s responsibility to document all the categories of data they collect and process.</p>
12.	<p>Q: How are NHS specific requirements regarding processing of sensitive data, including health records, addressed?</p> <p>A: Advanced has ensured full compliance with the 17 points mandated by NHS Digital in its “Information Governance Offshore Support Requirements”</p>

2.2	Governance and Compliance
1.	<p>Q: Do you have a published Data Protection policy?</p> <p>A: Yes, Advanced maintains a Data Protection policy. A copy of this can be provided upon request.</p>
2.	<p>Q: Do you have a published Information Security policy?</p> <p>A: Yes, Advanced maintains an Information Security policy. A copy of this can be provided upon request.</p>
3.	<p>Q: Do you have a Data Retention & Data Disposal policy?</p> <p>A: We are currently documenting our policies and processes in line with the GDPR compliance requirements.</p>
4.	<p>Q: Do you have policies/processes/procedures for the following areas:</p> <p>Acceptable Use</p> <p>Remote Access/Wireless</p> <p>Network Security</p> <p>Encryption</p> <p>Incident Response Management</p>

	<p>Change Management</p> <p>Vulnerability Management</p> <p>Anti-Virus</p> <p>Secure Software Development</p> <p>Security architecture</p> <p>Third party management</p> <p>Breach Notification</p> <p>Physical Security</p> <p>Personnel Security</p> <p>A: Yes, Advanced does have and maintains policies covering all the areas mentioned above. These are available to our staff on our corporate intranet or detailed in the Advanced Information Security Management Manual, where appropriate.</p>
5.	<p>Q. Is there a process in place to review and update these policies and procedures?</p> <p>A: Yes, As per our internal review process, documents are reviewed at least annually and after each major change.</p>
6.	<p>Q. How do you ensure awareness and compliance of your staff with these policies and standards?</p> <p>A: All new joiners are made aware of the relevant policies for their role as part of their induction program. People accessing new roles via promotion also have an induction process into the new role. In addition to this, Advanced performs regular refreshers course in sync with our ISO re-certification program (run yearly). Compliance is monitored and documented through various activities, including internal auditing, analysis of incidents and analysis of external audit outcomes. Additionally, all staff are required to undertake on-going Data Protection and Security Awareness training.</p>
7.	<p>Q: Are you willing to provide evidence to support your responses?</p> <p>A: Yes - subject to confidentiality obligations. Please contact your Account Manager at Advanced if you have any questions or concerns regarding this.</p>

8.	<p>Q: Are all these responses listed in this FAQ applicable to all the entities and sites your organisation will provide the services from?</p> <p>A: Yes – these responses are applicable to all the entities and sites within the Advanced Group.</p>
9.	<p>Q: Are your sites subject to regular certification audits?</p> <p>A: Yes, Advanced sites are regularly subject to ISO 27001 audit and certification. All of our sites in India were certified in September 2017. Advanced sites in the UK and India are regularly audited, by BSI, against ISO 27001:2013 to a frequency compliant with UKAS requirements</p>
10.	<p>Q: Do you maintain and update records of processing activities that can be used to demonstrate that you are using the data only for the purpose agreed with the Data Controller?</p> <p>A: Advanced is in the process of creating records of processing activities as part of our GDPR Compliance Program.</p>
11.	<p>Q: Do you maintain and update Records of Processing Activities.?</p> <p>A: Yes. Advanced maintain records of processing activities – both as a Data Controller and Data Processor in compliance with Article 30 of the GDPR.</p>
12.	<p>Q: Do you have an archive and back-up policy?</p> <p>A: We are currently documenting the archive and back-up procedure in line with the GDPR requirements.</p>
13.	<p>Q: Do you have User Access control policy in place?</p> <p>A: Yes. Advanced has an Access Control Policy which is currently being aligned with the GDPR requirements.</p>
14.	<p>Q: Do you have a well-defined Leavers process in place to ensure that all access for the terminated employees is revoked?</p> <p>A: Yes. Leavers' notification is sent out in a timely manner to the Business teams in order to ensure all access is revoked no later than the termination date.</p>
15.	<p>Q: Do you have a Safe and Strong Password Policy in place?</p> <p>A: Yes, this supported by technical controls through active directory and documented in the Acceptable Use Policy.</p>
16.	<p>Q: If requested, can a representative of the Data Controller visit your facilities to observe and assess the physical controls in place?</p>

	A: Yes, by prior arrangement and mutually agreed dates/times. Please note, a suitable photo ID and a written authorisation letter on the customer's company letterhead will be required prior to any visits.
--	--

2.3	Supplier / Third Party Management
1.	<p>Q: Do your contracts with sub-contractors integrate the same data protection clauses as your contract with the data controller?</p> <p>A: Yes – all sub-contractors are required to sign a NDA and/or supplier contract which includes requirements pertinent to data protection requirements.</p>
2.	<p>Q: Are contract/temporary workers subject to a vetting process?</p> <p>A: Contractors and temporary workers have the same full background checks that permanent staff are subject to.</p>
3.	<p>Q: Do you have a supplier assessment in place?</p> <p>A: Yes. All suppliers are vetted and authorized by a designated approver within Advanced as part of our supplier on-boarding process. Also, Advanced have a standard supplier questionnaire, which is completed as part of the supplier assessment.</p>
4.	<p>Q: How do you ensure that third parties comply with your data protection and information security policies?</p> <p>A: We are currently reviewing our procedures. In future, all third parties will be audited to ensure their individual staff members are compliant with data protection requirements.</p>

2.4	Personnel Security
1.	<p>Q: How many staff does your organization have?</p> <p>A: More than 2000 staff are currently employed by Advanced.</p>
2.	<p>Q. Do you perform background checks on your staff?</p> <p>A: All staff, both permanent and temporary, recruited within the Advanced group are vetted.</p> <p>All permanent and temporary staff in offshore offices are subject to the same rigorous security checks as our staff in the UK and this has been in place since 2014. These checks are initiated when the</p>

	<p>hiring manager has determined to offer an individual employment and are conducted by a locally-contracted organisation.</p> <p>The substance of the background checks are as follows:</p> <ul style="list-style-type: none"> • Address • Employment • Criminal Record • Education
3.	<p>Q: How do you ensure that your staff understand the information security requirements and practice non-disclosure?</p> <p>A: As part of our user awareness training program, we have a mandatory GDPR Awareness training for all staff. We conduct regular data protection and information security awareness training for new starters as well as existing staff. We are rolling out a GDPR awareness and training pack to third parties as well as part of our GDPR compliance program.</p>
4.	<p>Q: Do you have a mandatory Confidentiality agreement to be signed by all the employees, contractors and third parties?</p> <p>A: Each member of the staff signs a confidentiality agreement when employment contracts are signed.</p>
5.	<p>Q: Do you have a mandatory User Awareness & Training program for Information Security and Data Protection?</p> <p>A: As part of the Advanced induction process, staff undertake computer-based learning that covers Information Security. In addition, a further module is being developed to cover GDPR obligations and expectations which all staff will be offered.</p>
6.	<p>Q: Do you give specialised training to the users involved in the delivery of the services?</p> <p>A: Yes. All staff who are authorized to work in the remote access environment are trained in the requirements of Data Protection and Confidentiality, as well as appropriate procedures to ensure that:</p> <ul style="list-style-type: none"> • we have customers' authorization to allow access to their systems.

	<ul style="list-style-type: none"> where authorization is missing, obtain authorisation from customer via appropriate means such as Data Transfer Authorisation Form or Controlled Remote Data Access Form.
7.	<p>Q: What are the provisions for providing support, guidance and advice to the users for handling data and equipment?</p> <p>A: A DPO has been appointed to provide support, training and guidance to the staff across the Advanced group of companies.</p> <p>In addition, Advanced Health & Care has a Caldecott Guardian to advise staff regarding health and care specific guidelines.</p>
8.	<p>Q: Do users have direct access to the Data Protection Officer and the Information Security Officer?</p> <p>A: Yes – all existing employees across the group were informed when the DPO joined and anyone can easily reach out for advice and guidance via internal phone/email/skype. All new starters attend a mandatory Data Protection training which is delivered by the DPO. In addition, we have appointed Information Security Managers and a Caldecott Guardian who are available to provide advice and support where needed.</p>
9.	<p>Q: Are the users involved in the delivery of the service aware of your obligations as a Data Processor?</p> <p>A: A specialised and targeted training program has been rolled out to the users involved in delivering the Data Processor obligations and services to the customers.</p>

2.5	Organisation Standards
1.	<p>Q: How do you report security incidents to clients?</p> <p>A: Security incidents are reported to clients through the normal support process. All security incidents and platform wide issues are followed up with a Major Incident Report covering the nature of the incident, the resolution and any preventative action planned to avoid recurrence.</p>
2.	<p>Q: What is your organisation's process for disposing of computer equipment used in processing the data?</p>

	<p>A: Confidential, personal or client printed data is securely shredded or placed in confidential waste bins. Electronic equipment and media (including CD's, DVD's, USB devices, Tapes, Personal Computers, Phones, Tablets and Disks) are returned to the Advanced IT team for secure wipe and/or disposal.</p>
3.	<p>Q: How often is access to written or printed material and access to computer systems reviewed?</p> <p>A: Access to computer systems is reviewed monthly as part of Advanced's compliance with ISO 27001 requirements.</p>
4.	<p>Q: Please explain your audit procedure and schedule for vulnerability management activities and logs.</p> <p>A: Vulnerability scans are undertaken by the Advanced platform services team on a monthly basis in order to ensure vulnerabilities have not been introduced to the systems and the effectiveness of the patching cycles is maintained. System logs are maintained and reviewed as part of the vulnerability testing process.</p>
5.	<p>Q: On termination of the contract, how will the data be returned? Will any data be retained?</p> <p>A: Hosted Data: No data will be retained unless agreed in a bespoke contract. Data will be returned to the customer in a machine readable format, unless agreed otherwise in the contract.</p> <p>Data Processing Outside EEA</p>

	Data Processing Outside EEA.
--	------------------------------

3. Access to Customer Data and/or Network

This section is applicable to the Support Services and Hosting Services provided by Advanced and hence divided in two categories:

3.1	Support Services
1.	Q: Do you need access to our network for the delivery of the support services contracted to you? If yes, please specify the procedure.

	<p>A: From time to time Advanced will need to connect to customer sites to provide support, when this is required, Advanced use Screen Connect which is a secure method of connection. Other connection methods may be used depending on customer requirements.</p>						
2.	<p>Q: Where will the support services be provided from?</p> <p>A: Level 1 and Level 2 Support is provided from the UK. For Level 3 support, our UK team will work with our India operation to resolve incidents which may involve controlled remote access being provided to the India team to customer data which will be stored in the UK.</p>						
3.	<p>Q: Will you sub-contract any of the support services provided to us to a sub-processor?</p> <p>A: Yes, please see details of partners, listed below:</p> <table border="1" data-bbox="424 797 1430 1169"> <thead> <tr> <th>Sub-processor Name</th> <th>Services to be provided</th> <th>Lawful basis of data sharing</th> </tr> </thead> <tbody> <tr> <td>Advanced Business & Health Care Solutions, India Ltd.</td> <td>Incident resolution, Bespoke development, Problem resolution via controlled remote access only.</td> <td>Standard Contractual Clauses, GDPR compliant Data Protection clauses – signed with the sub-processor</td> </tr> </tbody> </table>	Sub-processor Name	Services to be provided	Lawful basis of data sharing	Advanced Business & Health Care Solutions, India Ltd.	Incident resolution, Bespoke development, Problem resolution via controlled remote access only.	Standard Contractual Clauses, GDPR compliant Data Protection clauses – signed with the sub-processor
Sub-processor Name	Services to be provided	Lawful basis of data sharing					
Advanced Business & Health Care Solutions, India Ltd.	Incident resolution, Bespoke development, Problem resolution via controlled remote access only.	Standard Contractual Clauses, GDPR compliant Data Protection clauses – signed with the sub-processor					
4.	<p>Q: What is the access control process in place with respect to the data shared by the customer with the support services?</p> <p>A: Access to the data (hosted in the UK) is controlled by UK resources who only grant access to resources in India on a role basis – i.e. Role-Based Access Control (RBAC) - using individual login details. Also, all staff in India are trained not to share any login credentials.</p>						
5.	<p>Q. Will all data shared by the customer with the support services be deleted if the contract is terminated and/or the customer stops using your product?</p> <p>A. All data related to specific incidents will be deleted when the incident or problem record is closed within Support. If the customer terminates the contract, any open incidents will also be closed and all related data will be deleted.</p>						
6.	<p>Q: How many staff will be involved in the delivery of the support services to the Data Controller?</p> <p>A: Advanced has over 300 members of staff in its support services.</p>						
7.	<p>Q: How many staff will have access to the Data Controller's data or network?</p>						

	A: Each support team is responsible for the support of between 1 and 5 products depending on the size and complexity, team size ranges from a few to 20 people.
--	--

3.2 Hosting Services

1.	<p>Q: Do you need access to our network for the delivery of the hosting services contracted to you? If yes, please specify the procedure.</p> <p>A: All Managed Hosting services are delivered from UK Data Centres. To provide some services in a secure way we may need the engagement of customer IT teams to implement site to site 256 bit encrypted VPN's, to connect customer networks in order to provide a secure tunnel for file transfer, printing or other services. In optional 'hybrid cloud' deployments, a local domain controller may also be part of a wider hosted domain forest.</p>						
2.	<p>Q: Where will the services be provided from?</p> <p>A: All Managed Hosting services are delivered exclusively from Data Centre facilities in England. Customer data is not transferred or stored outside of these facilities.</p>						
3.	<p>Q: Will you sub-contract any of the hosting services provided to us to a sub-processor or a supplier?</p> <p>A: A current list of sub-processors is specified below. However, depending on the software services contracted, further sub-processors may be used to enable the delivery of certain functionality. In such cases Advanced will undertake only lawful, contractually binding data processing and inform the Data Controller about new sub-processor at no less than 30 days' notice. Further details of these sub-processors are available on request via your Account Manager.</p> <p>A: Advanced Health & Care Customers:</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">Sub-contractor Name</th> <th style="width: 40%;">Services to be provided</th> <th style="width: 30%;">Lawful basis of data transfer</th> </tr> </thead> <tbody> <tr> <td>Level 3, Islington</td> <td>Data Centre Service, providing cabinets and services up to them, (not the equipment within)</td> <td>Contract</td> </tr> </tbody> </table>	Sub-contractor Name	Services to be provided	Lawful basis of data transfer	Level 3, Islington	Data Centre Service, providing cabinets and services up to them, (not the equipment within)	Contract
Sub-contractor Name	Services to be provided	Lawful basis of data transfer					
Level 3, Islington	Data Centre Service, providing cabinets and services up to them, (not the equipment within)	Contract					

Virtus, Slough	Data Centre Service, providing cabinets and services up to them, (not the equipment within)	Contract
<p>A: Customers, excluding Health & Care:</p>		
Sub-contractor Name	Services to be provided	Lawful basis of data transfer
Claranet UK	Data Centre Services Hardware Maintenance Data Backup Managed Services	Contract
Telstra Global	Data Centre Services Hardware Maintenance Data Backup Managed Services	Contract
4.	<p>Q: Will your organisation collect any data on behalf of the Data Controller?</p> <p>A: Advanced does not collect any data from customer's customers for its own processing purposes. However, for certain clinical software products, an optional service is available to allow certain data sharing with NHS Public Health England. This is for national clinical safety work, for example tracking flu outbreaks. The data is collected through Advanced only in the event that the customer signs a data sharing agreement.</p>	
5.	<p>Q: What is the access control process in place with respect to the hosted data?</p>	

	<p>A: Role Based Access controls are defined and in use, restricting access to the hosted systems. These are defined within our ISMS (Information Security Management System) policy.</p> <p>As per the process, access to the systems must be formally requested in writing, which is in turn reviewed by members of the platform support service prior to approval or rejection. For all client access requests, a case is logged onto the system for initial review. A proposal is then generated and sent electronically to a senior client representative who has the relevant privileges to be able to sign off on behalf of the company. Authorisation for access is signed electronically and sent back to Advanced for processing.</p>
6.	<p>Q: How do you ensure that users only have authorised access on the need to know basis?</p> <p>A: For Advanced employees, a standard joiners and leavers policy (as part of the HR induction process) ensures access to systems is closely monitored and controlled. Only those employees with approved authorisation to use the hosted systems are granted access as detailed in the Answer 5 above.</p>
7.	<p>Q: How do you ensure that the users are following the password guidance for the systems in the support environment?</p> <p>A: The hosted password policy is set with the Microsoft Windows Active Directory. Password complexity, length and reset period is mandated</p>
8.	<p>Q: How do you manage privileged access to the systems?</p> <p>A: Privileged access is only granted to authorised members within Advanced. All members with privileged access must have undergone relevant security checks; received the necessary security awareness training, and signed the relevant Acceptable Use Policy agreements prior to accessing any systems.</p>
9.	<p>Q: How many staff will have access to the Data Controller's data or network?</p> <p>A: There are more than 20 members of staff in the Hosting support team and over 70 at the Service Desk, Application Delivery and Database Admin teams, who will have access to the Data Controller's network and application/systems.</p>

4. Data Processing Outside EEA

This section is applicable to the Support Services and Hosting Services provided by Advanced and hence divided in two categories:

4.1	Support Services
1.	<p>Q: Do you process any data outside of the European Economic Area? If yes, please provide details of the data processing?</p> <p>A: We provide Level 3 Support Services from our offices in India. For this purpose, controlled and restricted remote access to the customer data is provided to the staff in India. Please note that on an average, the number of incidents that get escalated to level 3 are only 2% of the total incidents logged per month by the Support Services – based on the most recent statistics as of February 2018.</p>
2.	<p>Q: What is the relationship between Advanced UK and data processor outside EEA?</p> <p>A: Advanced in India is a separate legal entity that is part of the Advanced Computer Software Group Ltd. Whenever customer data will be accessed from Advanced in India, Advanced in the UK will be considered the Data Processor and Advanced in India will be the Sub-Processor with regards to the services provided to Advanced customers.</p>
3.	<p>Q: What is your lawful basis for sharing data with the Advanced in India?</p> <p>A: Advanced in the UK has signed a contract with Advanced in India that incorporates standard contractual clauses issued by the ICO (Information Commissioner’s Office) and also the data protection clauses compliant with the GDPR requirements.</p> <p>In addition Advanced has issued the Advanced Data Protection Addendum to all its customers which sets out the binding data protection clauses in compliance with the GDPR. The addendum clearly specifies that the Level 3 support will be provided via controlled remote access from India.</p> <p>In the instance where the Data Controller challenges the terms of the Data Protection Addendum and Support Services receive a call from the customer for logging a Level 3 incident, a Controlled Remote Data Access Form will be sent out to the customer to obtain consent to provide remote access to staff in India for the purpose of investigating and resolving the incident concerned.</p>
5.	<p>Q: What is the purpose of allowing controlled remote access to the data from India?</p> <p>A: The purpose for the controlled remote access is to enable the following tasks to be undertaken by Advanced in India:</p> <p>Level 3 support and incident resolution</p>

	<p>Advanced staff (software engineers) with the necessary skills to resolve Level 3 support incidents (namely: defects/issues and root cause analysis) are all based in our fully owned and managed operation in India. When an incident gets escalated to Level 3, controlled and restricted remote access will be provided to the authorised staff in India.</p>
6.	<p>Q: What will be the duration of data sharing?</p> <p>A: Controlled remote access to the data is awarded for particular incident number and terminates as soon as the incident is formally accepted as 'closed' by the client (data controller).</p>
8.	<p>Q: What will the data retention period be?</p> <p>A: When required for incident or problem resolution, Advanced will request data to be transferred from the customer to Advanced UK server by sending out a <i>Data Transfer Authorisation Form</i>. Under no circumstances can the data transfer to Advanced UK server exceed 10 working days without the Customer being informed and, if necessary, additional authorisation obtained.</p> <p>The controlled remote access provided to authorised users in India for Level 3 resolution will be terminated as soon as the Customer accepts the incident as closed. Any copies of the data that may have been transferred to the UK server for use by India will be deleted at the same time.</p> <p>Additionally, any screenshots or example cases shared by the clients with the Support Services for incident resolution, will be deleted from the email servers and defect resolution system (JIRA).</p>
10.	<p>Q: Is it possible to provide the services without allowing controlled remote access to the data from India?</p> <p>A: It may be possible to deliver part of the service without allowing controlled remote access to the data from India but there will be implications such as extended resolution time, added complexity in anonymising data, incomplete data to test support incident if parts are removed. We would discuss this on a case by case basis.</p>
16.	<p>Q: Will the data be sub-contracted to third parties by the facility in India?</p> <p>A: There are no third parties to whom any service has been sub-contracted in India. This has been incorporated in the contract between Advanced in the UK and Advanced in India</p>
17.	<p>Q: How will you monitor that Advanced in India is handling data in compliance with the data protection legislation?</p> <p>A: A mandatory training program is in place for all staff in India and the standard contractual clauses, issued by the European Commission, have been signed between Advanced in the UK and Advanced in India. When remote access to data is needed, the UK Level 2 support staff are able to see and control what data is being accessed by the Level 3 support staff in India as Advanced in the UK will provide controlled remote access to Advanced in India.</p>
18.	<p>Q: Can I communicate directly with the support/development staff in India?</p>

	<p>A: For the purpose of security and visibility, any instruction from our customers should be made to Advanced in the UK who will then liaise with the staff in India.</p>
--	--

<p>4.2</p>	<p>Hosting Services</p>
<p>1.</p>	<p>Q: Do you store hosted data outside of the European Economic Area? If yes, please provide details of the data processing?</p> <p>A: No. All hosted customer data is stored in the UK.</p>

5. Technical & Organisational Measures

This section is applicable to the Support Services and Hosting Services provided by Advanced and hence divided in two categories:

5.1	Support Services
5.1.1	Technical Security Controls
1.	<p>Q. Please provide an overview of the security controls in place at sites from where you provide support services.</p> <p>A: <u>Network Security</u></p> <p>Network Segregation: Our internal networks are segregated to restrict access to areas of the networks that contain sensitive data, with RBAC (Role Based Access Control) to further restrict access to specific individuals within certain roles.</p> <p>Firewalls: Advanced deploys a range of market-leading industry standard firewall appliances to protect the advanced internal network environment from malicious attack.</p> <p>Anti-virus and Anti-malware: Advanced use a variety of Leading third party products to ensure that all internal systems are protected with anti-virus and anti-malware, together with email processing and Web Protection against malicious websites.</p> <p>Patch Management: Advanced use an industry standard patching policy to ensure that software updates and security fixes are applied to our internal systems in a timely fashion, in line with vendors' recommendations.</p> <p>Monitoring and Logging: Advanced utilise a variety of market leading third party applications and platforms for the early identification of service degradation/failures, which are then triaged through appropriate channels.</p> <p>B: <u>Data Transfer Security</u></p> <p>Advanced uses industry standard SFTP platform for all data transfers from the customer to Advanced UK server.</p> <p>C: <u>Remote Access Security</u></p> <p>Advanced use Screen Connect for secure remote access connection to the customer network.</p>

5.1.2 Remote Access Security Controls - India	
1.	<p>Q: Is it secure to allow controlled remote access to data from India? What are the security measures in place?</p> <p>A: The Advanced operation in India is ISO27001 certified and thus has all the security measures in place as prescribed in the standard.</p> <p>In addition, Advanced deploys VPN and 256 bits encryption to all communication links between UK and India to mitigate the risk of interception by the third parties.</p>
2.	<p>Q: How will you control the remote access to data from India?</p> <p>A: Access to the data (hosted in the UK) is controlled by UK resources who only grant access to resources in India on a role basis – i.e. Role-Based Access Control, (RBAC) - using individual login details. In addition to this, all staff in UK and India have signed a Confidentiality Agreement with Advanced preventing them to discuss or share any information related to their work.</p>
3.	<p>Q: How will you prevent unauthorised access to the data?</p> <p>A: Access to the data (hosted in the UK) is controlled by UK resources who only grant access to resources in India on a role basis – i.e. Role-Based Access Control, (RBAC), - using individual login details. As staff in India are trained not to share any login credentials, there should be no risk of having un-authorised access to data.</p>
4.	<p>Q: Are the users in India aware of their data protection obligations?</p> <p>A: All staff members in India go through compulsory Information Governance and Information Security training as part of their induction process and regular refresher courses and tests are mandated.</p>
5.	<p>Q: Have you provided any training to the staff in India?</p> <p>A: All staff members in India go through compulsory Information Governance and Information Security training as part of their induction process and regular refresher courses and tests are mandated.</p>
6.	<p>Q: How will you monitor that the Sub-Processor (India) is handling data in compliance with the data protection legislation?</p> <p>A: In addition to the mandatory training attended by all staff in India and the legal clauses implemented between Advanced in the UK and Advanced in India. When remote access to data is needed, the UK Level 2 support staff are able to see and control what data is being accessed by the support staff in India as Advanced in the UK will provide restricted and controlled remote access to Advanced in India.</p>
7.	<p>Q: What are the security measures in place at the facility in India?</p> <p>A: <u>Access Control</u></p>

	<p>Access to the data (hosted in the UK) is controlled by UK resources who only grant access to resources in India on a role basis – i.e. Role-Based Access Control (RBAC) - using individual login details. As staff in India are trained not to share any login credentials, there should be no risk of having un-authorized access to data.</p> <p><u>Transmission Control</u></p> <p>All communication links between UK and India use VPN and 256bits encryption to mitigate any risk of interception by the third parties.</p> <p><u>Input Control</u></p> <p>Support staff in India only have access to copies of live data and/or copies of customer environment. Therefore there is no need to track data input or changes as these additions or modifications would only be done on “test systems” for the benefit of defects identification. These systems are then erased once the support task is completed.</p> <p><u>Job Control</u></p> <p>This is achieved by recording who requests access to the data and for what purposes in a tamperproof database (the records include a reference to the support ticket being worked on). Additional checks are done such as making sure that the person making the request is assigned to the products the request is made for and is on support duty/shift/assignment at the time the request is made.</p> <p><u>Availability control</u></p> <p>Only with customer’s authorisation will we grant controlled remote access to authorised users in India to view the data purely for incident resolution. Please refer to Answer 6 in Section 2.4 on details regarding this.</p> <p><u>Separation Principle</u></p> <p>Data access is only for support purposes, by formally agreed exception. No unauthorized copying or retention of data is permitted and all access is monitored. All staff are duly trained regarding our data protection obligations.</p>
--	--

5.2	Hosting Services
5.2.1	Physical Security – Data Centres

1.	<p>Q: How do you ensure there is no unauthorised access to the premises from where the services are provided to the Data Controller?</p> <p>A: The datacentre facilities are protected by CCTV monitoring in addition to qualified 24x7 security guard patrols from a reputable service provider employed by Advanced. Access control requires an access card, PIN and biometric identity check, with only zoned access granted. There is a fully controlled good-in and out procedure.</p>
2.	<p>Q: How do you ensure that the equipment and systems used to provide the services are not accessed by the unauthorised users?</p> <p>A: Security is provided by the Role Based Access Control (RBAC), with a process in place to assign rights based on need. Furthermore there is an application level security granting access rights only to the approved users.</p>
3.	<p>Q: Please describe your archiving procedure for the customer data in the hosting environment.</p> <p>A: All user data is backed up overnight, using a combination of full backup and incremental backup methodologies, with data held in an online digital archive for a minimum of 14 days.</p>
4.	<p>Q: Do you have an inventory of authorised devices and software?</p> <p>A: All assets assigned to individuals are recorded by Advanced's IT teams . Only registered assets are able to connect to Advanced networks.</p> <p>System assets, e.g. servers, routers, etc. are recorded and monitored by Advanced Group IT.</p>
5.2.2	<p>Network Security</p>
1.	<p>Q: Do you have a secure network architecture in place?</p> <p>A: Yes, the data centre network architecture is securely provisioned and administered with controlled ingress and egress points. External connectivity is encrypted.</p>
2.	<p>Q: Please provide details of the firewall software that will be used to protect the Data Controller's systems and data.</p> <p>A: Advanced deploys market leading next generation firewall appliances to protect the Private Cloud environment from malicious attack and can accommodate customer specific rules as necessary.</p>
3.	<p>Please provide details of the monitoring services and logs to detect malicious activity.</p> <p>A: Advanced runs a combination of different solutions depending on the environment. Firewall logs are written to a secure storage area which only staff with appropriate rights have access to. Network monitoring tools include:</p> <p>Nagios – provides advanced intelligent real time alerting on hardware based devices for many different criteria, which extends to various elements</p>

	<p>AppDynamics – identifies code execution times, showing up any hardware or software bottlenecks. This also drives code improvement.</p> <p>Zabbix – provides data on bandwidth utilisation for the internet and N3 connections.</p> <p>Solarwinds – Configuration management and capacity management.</p> <p>The Security Operations Centre (SOC) monitors alerts for selected systems and customers, depending on the service defined in the project scope.</p>
4.	<p>Q: Please provide details of intrusion prevention and/or data loss prevention systems in place.</p> <p>A: IPS and IDS are not currently in use, however threat management is controlled through Cisco firewalls. Data Loss is mitigated with high levels of platform resiliency, including SAN based storage and monitored backup regimes.</p>
5.2.3	Vulnerability Management
1.	<p>Q: Do you have security controls in place to ensure segregation of information between clients?</p> <p>A: Product types are separated based on connectivity requirements. Services on N3 networks have two layers network segregation from all other services. Data is controlled through logical separation, through Rights Based Access Control (RBAC) and VLAN's segregating product areas.</p>
2.	<p>Q: Do you have a routine vulnerability scanning for the systems to ensure protection against the vulnerabilities?</p> <p>A: Yes, vulnerability scans are implemented internally using industry standard tools.</p>
3.	<p>Q: What measures and controls do you have in place for vulnerability management of the network and network devices, such as firewalls, routers, and switches?</p> <p>A: Please see the answer above - this is complemented by the actions undertaken to maintain firmware as defined in the Hosted Patching Policy.</p>
4.	<p>Q: What is your patch management process?</p> <p>A: Please refer to the Service Description and Hosted Patching Policy.</p>
5.	<p>Q: What application security test reports will be provided to the Data Controller as part of the vulnerability management process?</p> <p>A: No reports are provided, application security test reports are confidential to the Advanced Product Management teams who will assess and prioritise the patching of vulnerabilities.</p>
6.	<p>Q: What anti-virus do you deploy on the systems and how often are these updated?</p> <p>A: There is a combination of McAfee and Forefront in use across the estate. These are automatically update as and when the manufacturers release updates, generally daily.</p>

7.	<p>Q: Please explain your process and procedure for penetration testing and disaster recovery testing.</p> <p>A: Advanced undertakes vulnerability scanning using the SAINT solution. Where disaster recovery options are available, data can be restored by Support into test areas and checked for data integrity. The frequency of this service will be defined in the contract at the point of ordering, if this service is purchased.</p>
<p>5.2.4 Data Transmission</p>	
1.	<p>Q: Please provide details of the secure encrypted protocols used to manage servers and network devices?</p> <p>A: Network devices are managed within a secure management network and servers are secured by firewalls. In both instances SSL/TLS secure encryption protocols are used.</p>
2.	<p>Q: How do you manage and control the use of ports, protocols and services on networked devices?</p> <p>A: The default policy is to deny all access. All ports, protocols and services are enabled based on need and only once the risk evaluated by the Change Advisory Board (CAB).</p>
3.	<p>Q: What type of authentication is required to access the servers and network devices both from on-site and remote access?</p> <p>A: The type of authentication varies depending on the system and software the customer uses. Typically all critical systems use Kerberos backed account security or Secure Sockets Layer/Transport Layer Security (SSL/TLS).</p>
4.	<p>Q: Please provide details of your remote access procedure for the employees and contractors.</p> <p>A: The procedure varies depending on the system and software the customer uses. Typically customers are provided a secure tunnel to the datacentre, or are provided SSL security where applications are delivered through web services.</p>
5.	<p>Q: How do you manage and control the flow of information between networks of different trust levels?</p> <p>A: All information flows are encrypted and directed to known servers. Before transmitting any live data outside of Advanced's controlled network into the customer environment, the standard procedure is followed. This involves sending out the dummy data first and receiving validation and confirmation of receipt of dummy data from the customer prior to transmitting the live data.</p>
6.	<p>Q: How is personal or sensitive data encrypted both in transit and in storage?</p> <p>A: Customers excluding Health & Care: The data stored on disk is not encrypted, but is held securely in SANs within the datacentre, in locked cabinets and high security zones. Customers can optionally upgrade to encrypted storage. Data in transit is always encrypted to a minimum standard of 256 bit.</p> <p>Health & Care customers: Virtual machine data resides on Advanced's shared storage arrays with logical volumes encrypted by default. Data in transit is encrypted to a minimum standard of 128 bit.</p>

	<p>Encryption Standard: When encrypted, data is protected by the Advanced Encryption Standard (AES) algorithm that uses a 256-bit symmetric encryption key in XTS mode, as defined in the IEEE 1619-2007 standard as XTS-AES-256. That data encryption key is itself protected by a 256-bit AES key wrap when stored in non-volatile form.</p>
7.	<p>Q: Will you be holding personal data belonging to the Data Controller on its own server or a cloud server? In case of cloud server, please confirm the geographical location of this server?</p> <p>A: All customer data is stored on logically separated storage arrays on one of the aforementioned Cloud platforms, and this would be recorded in your service description. All data is stored in the UK.</p> <p>Customers excluding Health & Care Advanced utilise Telstra, Claranet and Advanced Cloud platforms to store data.</p> <p>Health & Care Customers: Advanced store data on equipment we own held within London datacentres.</p>