t: 01844 858 858 e: hello@intuitiv.net w: www.intuitiv.net

Author

Cormac Murphy

Owner

Data Protection Officer

Subject

Policy Statement And Agreement For The Provision Of Data Processing Services

Classification

1: Internal / Client

Version

1.1

Date

22 February 2018

Review date

22 February 2019

POLICY STATEMENT AND AGREEMENT FOR THE PROVISION OF DATA PROCESSING SERVICES

Revision history

Revision date	Previous version	Reviewer	Description
1	N/A	Cormac Murphy	First Version
1.1	1	Cormac Murphy	Added section detailing encryption requirement for data in transit. Updated links to ICO documents.

Contents

1 Summary

The below document defines the basis on which Intuitiv Ltd is prepared to enter into an agreement with a Data Controller as their Data Processor, where Intuitiv can be defined as the Data Processor, and what contractual clauses, responsibilities and liabilities Intuitiv is prepared to have included within such agreements.

2 References

This document has been created in consultation with the following documents from the UK Information Commissioners Offices (ICO):

Guide to the General Data Protection Regulation (GDPR):

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr

ICO GDPR guidance: Contracts and liabilities between controllers and processors:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/

Specifically, it has been built primarily according to the guidance provided by the ICO in the following document:

https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf

Which is also attached to this document as an appendix:

Appendix 1: ICO GDPR guidance: Contracts and liabilities between controllers and processors

3 Background.

GDPR (General Data Protection Regulation) will apply in the UK from 25 May 2018.

Intuitiv Ltd have been designing, building and hosting websites and web applications on behalf of their customers since approximately 1998. In this time, we have provided a very wide variety of bespoke solutions, which pre-date data protection requirements and responsibilities set out in more recent regulations.

As a provider of bespoke developed systems, these are built and delivered to the customers required specification at the date of commissioning the system. On payment for the developed system, Intuitiv release all ownership and intellectual property rights to that system to the customer. From this point onwards, any ongoing software application updates to the system (including data security updates) require further engagement of Intuitiv by the client, with further enhancements being delivered on the same bespoke development basis. Intuitiv do not develop or support “off-the-shelf” software, and do not provide any software maintenance contracts, nor raise any maintenance or support charges to ensure applications remain regularly updated on an ongoing basis. Intuitiv do raise hosting charges, purely to provide an internet hosting service for websites or web applications, but this does not include any provision for application updates.

It is therefore entirely possible that legacy applications will need attention to ensure the Data Controller (the customer owning the website) is compliant with the new GDPR. As bespoke systems, these will typically have been developed to the requirements of the client at the time of commissioning the systems, and as such, Intuitiv Ltd are unable to assume responsibility of ensuring they remain compliant with subsequent regulatory requirements.

Intuitiv Ltd do not position ourselves as experts on all the requirements of GDPR, particularly due to the complexity & broad scope of the new legislation, and also because it is still an evolving set of regulations. This, coupled with the fact the Data Controller will have more understanding of how their data needs managing, means Intuitiv will need to work closely with the controller and other third parties in defining how to respond to the introduction of the new regulations. Intuitiv Ltd are happy to provide “best efforts” advice on GDPR compliance, but this should not be relied upon to be definitive guidance, and where the controller is not able to rely on their own understanding of the regulations, expert advice should be sought from a suitably qualified third party.

Some changes to the Data Controllers systems may involve significant time and expense, which may result in these changes being effected after the introduction of the GDPR legislation. Where these changes are too onerous, consideration may be given to adopting completely new systems.

All works undertaken by Intuitiv Ltd to address GDPR requirements will be at the Data Controllers expense, and charged at Intuitiv Ltd’s standard rates.

Intuitiv Ltd are unable to guarantee all GDPR remedial work can be completed within the launch of the new legislation. Intuitiv Ltd has accrued a large customer base, and will schedule any GDPR works on a “best efforts” basis.

Going forward, for new developments after the introduction of GDPR, Intuitiv Ltd will similarly require the full involvement of the Data Controller and any expert third parties in ensuring new systems are GDPR compliant.

GDPR is an evolving specification, still not finalised at the date of writing this document, so all details contained herein are subject to change in line with legislation changes.

4 Are Intuitiv the Data Processor?

Intuitiv can only be classified as, and will only assume the “Main” or Primary Data Processor responsibilities where it designed, developed, deployed and host a website or web application on behalf of the Data Controller.

Where Intuitiv have been engaged by the Data Controller purely to provide hosting services, and have not been actively involved in all aspects of the design, development and deployment of the Website or Web Application involved, Intuitiv cannot be classified as the “Main” Data Processor. As a host of any system, Intuitiv may assume limited responsibilities as providers of the hosting platform, to be reviewed on a per case basis.

Intuitiv will not possess awareness or knowledge of how the website or web application and any of the data that it holds or processes has been designed or built, nor any of the security measures adopted in these system to ensure the compliance and security of the system and its data. As such, Intuitiv cannot be classified as the main or sole Data Processor.

In this scenario, the main Data Processor is the organisation who provided , developed and / or, is responsible for the website or web application, and all GDPR requirements should be directed to this organisation.

Intuitiv are a Data Controller only for data Intuitiv hold purely for its own organisational management, and this is addressed in a separate document, available on demand to relevant and authorised parties.

5 What responsibilities and liabilities do controllers have when using a processor?

- Controllers must only use processors which are able to guarantee that they will meet the requirements of the GDPR and protect the rights of data subjects.
- Controllers must ensure that they put a contract in place which meets the requirements set out in this guidance.
- They must provide documented instructions for the processor to follow.
- Controllers remain directly liable for compliance with all aspects of the GDPR, and for demonstrating that compliance. If this isn't achieved then they may be liable to pay damages in legal proceedings or be subject to fines or other penalties or corrective measures.

6 Contractual Agreement

This section defines the clauses which should be included in the contractual agreement between the Data Controller and Intuitiv Ltd, in the event that Intuitiv Ltd are to act as the Data Processor.

Included beneath each of these is additional detail that will need including and acknowledging within the contract.

6.1 Parties

(1) …….. – The Client, whose offices are at …….. (the "Data Controller");

And

(2) Intuitiv Ltd of The Royal Oak, 2 Bridge Road, Ickford, Bucks, HP18 9HX (the "Data Processor")

6.2 Compulsory Agreement Clauses

In accordance with guidelines from the Information Commissioners Office (ICO), the contract should contain the following minimal clauses.

6.2.1 The Data Processor shall only act on the written instructions of the Data Controller (Article 29);

All requirements of Intuitiv should be submitted by the Data Controller in written instructions, ideally email, with all relevant parties included in the recipient or cc list. Intuitiv are not able to accept verbal instructions, either in person or via voice or video call, without a follow up confirmation in writing.

The Data Controller is obliged to ensure that all instructions submitted to Intuitiv are fully compliant with all requirements of the GDPR.

6.2.2 The Data Processor must only engage a sub-processor with the prior consent of the data controller and a written contract (Article 28.2);

Intuitiv Ltd typically only engage full time, permanent members of staff in the provision of all its services, so engaging of sub-processors is highly unlikely. In the unlikely event this does occur, Intuitiv Ltd will only do this with prior consent from the Data Controller and a written contract between Intuitiv Ltd and the sub-processor.

This clause shall only apply where the Data Processor (Intuitiv Ltd) wishes to engage a sub-processor completely independently of the Data Controller. Where a sub-processor is either proposed by or engaged by the Data Controller, with instruction to work with Intuitiv Ltd, the Data Controller shall remain fully liable for all contractual engagement & responsibility for the sub-processor.

6.2.3 The Data Processor will ensure that people processing the data are subject to a duty of confidence;

Intuitiv Ltd engages permanent, full-time members of staff, all of whom are subject to a comprehensive on-boarding process, including:

- Signing a comprehensive Intuitiv Ltd contract of employment
- A basic disclosure check (DBS) of personal information, proof of identity, right to work check and criminal convictions check, which is carried out by the government organisation: Disclosure Scotland
- Induction and training on all Intuitiv policy and procedure compliance literature, which includes extensive data security instruction.
- Completion of a “Compliance Checklist”, confirming all training completion.
- Checked against UK government Sanctions List

Intuitiv Ltd has a comprehensive library of infrastructure, systems security, software development, data protection and policy and procedure compliance documentation, which defines how we as an organisation ensure the security of our systems, and the data they contain and process.

All Intuitiv Ltd employees are provided with induction and ongoing training in all documentation relevant to their job role. All employees complete a “Compliance Checklist” annually, to validate completion of this training.

This documentation contains company confidential information, which can provide significant insights into the operation of the business, its employees, its security measures and supporting systems. As such, Intuitiv Ltd are happy

to provide visibility of this documentation to contracted clients, but will require completion of a non-disclosure agreement to protect the information contained therein.

6.2.4 The Data Processor must take appropriate measures to ensure the security of processing;

Intuitiv Ltd have implemented robust, industry standard security measures, to protect our all IT systems and data, including, but not limited to:

- All core network routers implement comprehensive access list security
- All internet facing connections are protected by dedicated firewall appliances
- Firewall appliances additionally implement automated threat detection
- All servers implement a second level of defence in the form of software firewalls
- All servers are monitored 24/7 using automated software
- All relevant network events are recorded in syslog
- Geographically distributed hosting facilities
- Load balanced, replicated & mirrored systems available
- Remote access is locked down by either fixed IP address or VPN connectivity
- All user accounts & access rights managed by Microsoft active directory
- Strict segregation of duties within user groups including separation of administrator privileges
- Anti-virus software installed on all relevant hosts, with automatic scanning and definition updates
- Centrally managed software update distribution ensuring timely and controlled update process
- Data Leakage Prevention (DLP) software installed on all workstations
- USB / external devices disabled on all workstations
- Segregated WiFi network for mobile devices
- Wholly owned Disaster Recovery office facility with defined Disaster Recovery procedures
- Extensive physical security covering all locations, including CCTV and police monitored intruder & security systems

- Backup power systems
- Irretrievable physical destruction of all end of life data storage devices
- All security related processes reviewed and revised if needed on a minimum of an annual basis
- All staff training and compliance is refreshed on an annual basis. All employees complete a "Compliance Checklist" annually, to validate completion of this training.

As above, extensive additional information is available on all Intuitiv data security policies and procedures, but contains extensive company confidential security information, so can only be provided subject to a binding Non Disclosure Agreement.

6.2.5 The Data Processor must assist the Data Controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;

The GDPR provides the following rights for individuals ("data subjects"):

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

It is the Data Controllers responsibility to manage all communications (including but not limited to "Data Subject Access Requests") with the individual as to how these rights are requested and processed. Intuitiv will not directly process these requests on behalf of the Data Controller.

Intuitiv Ltd typically provides access to the data their systems hold via bespoke content management or "admin" systems. These usually offer access to the data contained, via a secure web browser interface, that allow the Data Controller to search for and access full details of the data held, and then perform any data processing operations required on that data. It may be these "admin" systems already provide sufficient function to satisfy some or all of

these requests, and this would typically be the most effective way of satisfying this requirement and allow the Data Controller to manage these requests independently of Intuitiv Ltd.

Where additional functional enhancements are required to these "admin" systems , the Data Controller will be required to provide a detailed technical specification of any functional requirements, Intuitiv Ltd will provide time and cost estimates to implement, and on acceptance, schedule as fits other development commitments already made.

Where these rights requests are more ad-hoc or cannot be simply processed by a management system, Intuitiv Ltd will provide time and cost estimates to retrieve, update , delete and process data via manual means.

Intuitiv will make "best efforts" to accommodate all requests in timeliness with GDPR requirements, but these will vary depending on the complexity of satisfying the data requirement.

Where Intuitiv have been engaged purely to provide a hosting service, and have had no active involvement in of the design, development and/or deployment of the website or web application, Intuitiv cannot be classified as the main Data Processor for the website or web application involved. All requests for assistance in responding to data requirements will need to be addressed to the organisation who designed, developed and/or deployed the website or web application.

6.2.6 The Data Processor must assist the Data Controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;

The GDPR requires that data breaches (loss of data, whether malicious or not) must be reported to the relevant Data Protection Authority within 72 hours of discovery.

An important statement here is that this is within 72 hours of discovery. Once Intuitiv become aware of a data breach having occurred, Intuitiv will alert the Data Controller within required timescales, but the actual breach itself may have occurred before becoming aware, in which case, Intuitiv are unable to provide notification from the point of the breach itself.

Intuitiv will provide all detail it possesses of the breach to the Data Controller, including a data protection impact assessment, but the Data Controller then retains responsibility for reporting the Data Breach to the relevant Data Protection Authorities and to all affected customers whose data may have been compromised.

Intuitiv are unable to deal directly with either end users or the Data Protection Authorities on behalf of the Data Controller.

The nature of many website and web applications is that they provide access to the data they contain, via a wide potential variety of channels – including, but not limited to content management systems, "admin" systems, user portals, APIs (Application Programming Interfaces), and remote access protocols and clients. These are typically

provided by Intuitiv to the Data Controller, its staff, or other related third parties on instruction or agreement with the Data Controller, along with security and credential information to access these. Once provided, it is the responsibility of the Data Controller to ensure these channels are used in a secure and appropriate manner, and access details are managed in compliance with the relevant security best practice guidelines.

Where Intuitiv have provided any such or similar access to the Data Controller, or to any staff or other third Party on request by the Data Controller, it is essential that any investigations of data leakage also include a focus by the Data Controller on whether this leakage could have originated from a compromised or mis-used channel.

Intuitiv will not accept any responsibility for any data leakage where this loss may have resulted from inappropriate use of any such channel. Further to this, Intuitiv will only accept responsibility where it can be clearly identified that any leakage was due to an Intuitiv specific fault in the provision of its services.

Where Intuitiv have been engaged purely to provide a hosting service, and have had no active involvement in the design, development and/or deployment of the website or web application, Intuitiv cannot be classified as the main Data Processor for the website or web application involved. All responsibility for data security will remain with the organisation who designed, developed and/or deployed the website or web application.

6.2.7 the processor must delete or return all personal data to the controller as requested at the end of the contract;

Intuitiv will require a clearly specified written instruction from the Data Controller, detailing all data to be either deleted and / or returned, and an acceptance that once this occurs, Intuitiv no longer have any responsibility for the provision of any services related to that data, or liability for the data.

Intuitiv will typically provide data in the “native format” in which it is held in its systems, via simple download facilities.

Where the Data Controller requires this data is provided in an alternative format, particularly where this then requires processing of that data, Intuitiv reserve the right to levy reasonable charges for any work involved. Additionally, Intuitiv reserves the right to levy reasonable charges for any other costs related to providing access to or the delivery of the data.

An exception to this general rule applies if the Data Processor (Intuitiv) is required to retain the personal data by law.

Where Intuitiv have been engaged purely to provide a hosting service, and have had no active involvement in of the design, development and/or deployment of the website or web application, Intuitiv cannot be classified as the main Data Processor for the website or web application involved. All requests for assistance in responding to data requirements will need to be addressed to the organisation who designed, developed and/or deployed the website or web application.

6.2.8 the processor must submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

Intuitiv are happy to submit to any audits and inspections, at the request of the Data Controller. Intuitiv will require reasonable advanced notice of these audits and inspections occurring, and detailed written documentation of all activities associated with these requirements including timescales involved.

Where these audits and inspections have any significant time, resource or costing implication, Intuitiv reserve the right to pass any costs involved onto the Data Controller. In this case, Intuitiv will provide a costed proposal document for complying with the requirement, and on acceptance by the Data Controller, will schedule any activities involved.

Where any audits or inspections require access to company confidential information, Intuitiv will require that a Non-Disclosure Agreement is drawn up between all involved parties, committing those parties to keeping all information confidential and make use of this solely for the purposes of the audit or inspection.

As already detailed, Intuitiv are not experts in the interpretation of the GDPR, so will exercise best efforts in ensuring that it is not being asked to undertake anything that infringes the GDPR or other data protection law of the EU or a member state, based on Intuitiv's understanding of these requirements.

As such, it remains the responsibility of the Data Controller to ensure any requests it makes of Intuitiv are in compliance with all relevant regulations.

6.3 Additional Contractual Requirements.

These are not directly insisted upon in the ICO Guidance, but implied, and required for completeness.

6.3.1 Data Classification.

The GDPR requires Data Controllers ensure all data held is fully classified.

In order to respond to all its GDPR responsibilities, it is essential the Data Controller has a comprehensive understanding of all data held on its behalf, and the nature of processing of that data. As such, it is imperative that a Data Classification exercise is completed on all data held.

In order to support this, Intuitiv Ltd shall provide to the Data Controller, on their request, access to all data held on behalf of the Data Controller. This will typically be provided as a secure database connection, backup file or data schema, which will provide the Data Controller with visibility of all data it owns. The Data Controller shall then provide comprehensive data analysis documentation to the Data Processor that will:

- Classify all data held including categorisation of Data Subjects

- Clearly identifying what constitutes Personal Data and / or Sensitive Data
- Confirm Personal Data has been gathered with explicit consent from the Data Subjects
- Confirm Personal Data has been gathered under a lawful basis, respecting any applicable privacy policies and in line with all terms and conditions of engagement
- Specifying reasonable Retention Periods for all data. Data should only kept for as long as can be reasonably be expected to provide the business service requested
- Defining actions to be undertaken to protect data
- Defining actions to allow secure removal of unwanted data or data beyond its reasonable retention periods
- Define and restrict the types of processing that you authorise the Data Processor to perform on the data
- Any other appropriate data considerations

Intuitiv Ltd shall assume the Data Controller has familiarity with all aspects of any IT system Intuitiv Ltd has supplied, built or maintained on their behalf, and will require the Data Controller to provide comprehensive technical specification documentation, detailing any modifications required to these systems, in order to ensure compliance with the GDPR Guidelines.

Intuitiv Ltd shall then be provided reasonable time to analyse requirements, scope and provide a costed proposal document to address any issues or requirements arising from this Data Classification exercise. On acceptance of the proposal by the Data Controller, Intuitiv will then schedule the works agreed.

6.3.2 Documentation of Data Processing Activities.

The Data Controller should maintain their own independent documentation of all processing activity that is performed on their data, or data held on their behalf. This should comprehensively define the nature and purpose of all Data Processing performed on a Data Subject, so the Data Controller can respond independently to any Data Subject enquiries.

The Data Controller is responsible for confirming data is processed lawfully, fairly and transparently, and in a manner that ensures its security.

Intuitiv assume that the Data Controller is familiar with all aspects of the processing activity that is performed on their data, and this has been agreed when commissioned by the Data Controller, along with any relevant systems requirements specified. Where this is not clear to the Data Controller, Intuitiv may be able to assist in clarifying any

details that Intuitiv are fully aware of, but any time and cost involved in providing this detail may be subject to a chargeable rate.

The GDPR provides exemption for small and medium-sized organisations, having less than 250 employees. Intuitiv fall within this category, and as such are only obliged to document processing activities that:

- are not occasional; or
- could result in a risk to the rights and freedoms of individuals; or
- involve the processing of special categories of data or criminal conviction and offence data

Intuitiv hold a variety of records internally to document exchange and processing of data activity, including but not limited to:

- Information Asset Register
- Data Supply Log
- Email communications documenting data and processing activities

These records are private and confidential to Intuitiv, and contain security information that cannot be released to data subjects. The Data Controller should not rely on the availability of such data from Intuitiv limited to satisfy or respond to any Data Subject enquiries. The Data Controller should maintain their own independent records of Data Processing Activities so that they can respond to Data Subjects directly, and without recourse to Intuitiv.

6.3.3 Terms and Conditions of Personal Data Collection and Processing.

It is essential that any website or web application that collects and / or processes personal data has clearly defined and legally water-tight documentation detailing how all activity is performed in strict compliance with the GDPR guidelines. This is typically presented as:

- Terms and Conditions of Engagement
- Privacy Policies

Before any data is collected or processed, it is necessary to gain explicitly stated agreement from the Data Subject that they have read and understood the appropriate information, and are in agreement that their data may be collected on this basis. This is typically achieved by requiring the active checking or selection of an “opt-in” box accepting all terms stated, prior to any data collection of processing.

It is the Data Controllers responsibility to ensure all such agreements detailed on their website or web application comprehensively define all data collection and processing, are legally binding, and are in complete compliance with all requirements of the GDPR.

GDPR requires the agreement between Data Controllers and Data Subjects contain the following minimal commitments:

- The Data Subject has been informed who you are, how the data is processed, what other parties it is disclosed to
- Data has been collected for specific, explicit and legitimate purposes
- Data collection is adequate, relevant and limited to what is necessary for processing
- Consent to store and process data has been explicitly obtained
- Data is kept accurate and up to date
- Data is kept in a form that allows identification of data subjects only as long as necessary for processing
- A data retention policy is available, identifying a systematic way of destroying no longer needed data
- Data can only be archived for legitimate public interest , research and statistical, or legal and tax requirements
- Data is securely captured, transmitted and stored.

All personal, sensitive or confidential data collected by, and transmitted to or from any website should do so using encrypted HTTPS protocols, using secure cipher combinations. This is achieved by the registration of a Digital Certificate, which has been authenticated to ensure it matches the details of the legal entity who are the data controller for the website concerned. This can be verified by ensuring all webpages that transmit this data are served over a URL that is prefixed with “https://” and show a secure padlock symbol. Intuitiv offer digital certificate registration and renewal from a variety of issuers on request.

Intuitiv are not GPDR experts, or legally qualified to provide definitive advice or documentation guaranteeing compliance, and will rely on the Data Controller providing all documentation that requires deploying to the website or web application to ensure this compliance.

Intuitiv shall provide any content deployment or functional changes to support this compliance at its standard chargeable rates.

6.3.4 Penetration Tests and Security Audits.

To ensure the compliance and security of websites, web applications, and all the data held by these systems, it is imperative that these systems are subjected to regular penetration tests and security audits, and the results of these are addressed / acted upon in a timely manner.

Intuitiv Ltd is not a cyber security specialist. Intuitiv are a website design, build and hosting agency, and in providing these services we make best efforts to ensure all our staff are regularly trained in and kept up to date with all relevant security considerations, and our systems are built in compliance with the latest security best practices.

Commissioning of comprehensive penetration tests and security audits needs to be undertaken with an organisation that is a specialist in cyber security services. The work and costs for these services is not included in any charges raised by Intuitiv, and should not be construed to having been completed as part of a web application build or hosting service.

Intuitiv strongly recommend that all web applications built and hosted by Intuitiv are penetration tested and security audited by an independent third party, typically on an annual basis. Intuitiv are happy to recommend cyber security specialists, or work with any other supplier preferred by the Data Controller.

This is important for all web based systems, but particularly so for legacy systems that may have been designed and built prior to the latest data security protection requirements and regulations, and the ongoing emergence of new system vulnerabilities.

Where Intuitiv have been engaged purely to provide a hosting service, and have had no active involvement in of the design, development and/or deployment of the website or web application, Intuitiv cannot assist in making any software fixes to these systems. Intuitiv's responsibility is limited purely to addressing any infrastructure or hosting issues identified. All requests for assistance in addressing website or application software issues will need to be addressed to the organisation who designed, developed and/or deployed the website or web application.

Where a Penetration Test or Security Audit provides any advisory guidance for data security improvements to a website, application or hosting service, and Intuitiv have designed, developed and host the system involved, Intuitiv will then provide a costed proposal to remediate any issues highlighted, which will need to be accepted by the Data Controller before being scheduled for work.

6.3.5 nothing within the contract relieves the processor of its own direct responsibilities and liabilities under the GDPR; and reflect any indemnity that has been agreed.

Intuitiv have clearly specified "Terms of Business" under which it agrees to provide all services. This can be found on our website at:

https://www.intuitiv.net/terms-of-business

All email and proposal communications from Intuitiv Ltd are bound by the terms of this agreement.

Additionally, where website, application or data hosting is provided, Intuitiv provide a Web Hosting Service Level Agreement, which is available on demand.

These agreements, and any limitation of liabilities contained therein supersede any other agreement with the Data Controller.

Intuitiv will not assume any liability for websites or web applications where these have been designed, built and/or deployed by another organisation, and will not be classified as the main Data Processor in this scenario.

6.3.6 Data Storage Locations.

All data held by Intuitiv Ltd will be stored in the United Kingdom, subject to local UK government jurisdiction, at either:

1. Primary / High Availability Data Centre – London Telehouse Docklands, London
2. Backup / Disaster Recovery / Secondary Data Centre – Loudwater, High Wycombe
3. Head Office – Ickford, Buckinghamshire

Intuitiv Ltd hold all data within its own wholly owned and managed IT Systems. Intuitiv Ltd does not use third party or cloud hosting services for the storage of client data.

6.3.7 Data Protection Officer.

Intuitiv Ltd's Data Protection Officer is Tom Gould

In compliance with the GDPR requirement for Intuitiv Ltd to only act on written instruction (from the Data Controller, Data Subjects or any other Party), please submit any Data Protection enquiries to:

Email: dpo@intuitiv.net

Note: Intuitiv Ltd are unable to act as Data Protection Officer for anyone other than Intuitiv Ltd.

6.4 Agreement.

The Data Controller accepts all obligations in this agreement in consideration of the Data Processor continuing to provide its services.

This Agreement shall be governed by the laws of England and Wales.

SIGNED for and on behalf of …… (the "Data Controller") by:

Print Name: ……..

Position: ……..

Signature: ……

SIGNED for and on behalf of Intuitiv Ltd (the "Data Processor") by:

Print Name: ……..

Position: ……

Signature: ……..

7 Appendix 1: ICO GDPR guidance: Contracts and liabilities between controllers and processors

ICO GDPR guidance: Contracts and liabilities between controllers and processors