Just Surveys Ltd
Specialists in Drain Surveys

Dexters 1, Linton Farm Highnam,

Gloucester Gloucestershire, GL2 8DF

INTERNATIONAL DATA TRANSFER POLICY

Revision History

Version	*Revision Date*	*Revised by*	*Section Revised*
Version 1	25th May 2018	Barrie Haysman	The entire document

Document Control

Document Owner:	***Document No:***	***Status:***	***Date Approved:***
Julia Frith	*GDPR F205*	Approved	*25th May 2018*
Security Classification:	***Next Review Date:***	***Version:***	***Department:***
High	*25th May 2019*	*V1*	*Human Resources*

Table of Contents

1 POLICY STATEMENT

Just Surveys Ltd *(hereinafter referred to as the **"JSL")*** understands that any transfer of personal data undergoing processing or intended for processing after transfer to a third country or an international organisation, shall only take place in compliance with Chapter 5 of the GDPR.

This policy is to be read in conjunction with our ***Data Protection Policy*** and provides our procedures for transferring personal data to a third country or international organisation. We adhere to the Regulation for all non-EU transfers and have robust transfer safeguarding measures and controls in place to protect the personal data and the rights of the data subject.

2 PURPOSE

The purpose of this policy is to provide our procedures and guidelines for transferring personal data outside the EU for processing and to demonstrate our adherence to the Chapter 5 requirements and compliance with the required safeguarding measures.

JSL takes proportionate and effective measures to protect personal data held and processed by us, however we recognise the high-risk nature of disclosing and transferring personal data to a third country or an international organisation. This policy outlines the measures and controls that we take to comply with the data protection laws and provides guidance on transfer to our employees and associated third-parties.

3 SCOPE

This policy applies to all staff within JSL *(meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with JSL in the UK or overseas).* Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

4 OBJECTIVES

It is JSL's aim to ensure that all personal data transfers to a third country or an international organisation comply with the Chapter 5 requirements under the GDPR and that we ensure that data subject rights are enforceable and upheld. JSL has the below objectives regarding non-EU data transfers: -

- To comply with GDPR Articles 44-50 regarding personal data transfers to a third country or an international organisation
- To have adequate and appropriate safeguards and measures in place to protect personal data and data subjects when transferring personal information
- To only transfer data outside the EU where there is an adequacy decision by ***the European Commission*** *(hereinafter referred to as 'the Commission'),* one or more of the appropriate safeguards are place or the transfer complies with one of the transfer exceptions
- To have compliant Binding Corporate Rules or Standard Data Protection Clauses (*where applicable*) when transferring personal data without an Adequacy Decision
- Ensure that the DPO regularly reviews the Official Journal of the European Union to ensure that JSL's adequacy decision list is accurate and up-to-date

- To train and support all employees involved in personal data transfers to a third country or an international organisation
- To have robust and compliant policies and procedures in place for effecting non-EU transfers
- To regularly review and monitor this policy and any associated procedures

5 GUIDELINES & PROCEDURES

Where data is being transferred for a legal and necessary purpose, compliant with all Articles in the Regulation, we utilise a process that ensures such data is encrypted with a secret key and where possible is also subject to our data minimisation methods.

We use approved, secure methods of transfer and have dedicated points of contact with each Member State organisation with whom we deal. All data being transferred is noted on our information audit so that tracking is easily available, and authorisation is accessible. The Data Protection Officer authorises all EU transfers and verifies the encryption and security methods and measures.

5.1 ADEQUACY DECISION

Where we intend to transfer personal data to a third country or an international organisation, we check if the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection.

Where a positive adequacy decision is in place for the transfer recipient, we recognise that we do not require any specific authorisation to transfer the personal data and that the Commission has already undertaken a comprehensive assessment of the organisation or third country in making their decision.

Such transfers are still subject to our own security and encrypted transfer measures and safeguards and we still complete third-party due diligence where applicable. Such transfers are reviewed by the DPO and carried out following the same process as those within the EU.

The DPO is responsible for monitoring the approved third country list provided by the Commission and only transferring data under this provision to those countries, organisations or sectors listed.

5.2 APPROPRIATE SAFEGUARDS

In the absence of a decision by the Commission on an adequate level of protection by a third country or an international organisation, we restrict transfers to those that are legally binding or essential for the provision of our business obligations or in the best interests of the data subject. In such instances, we develop and implement appropriate measures and safeguards to protect the data, during transfer and for the duration it is processed and/or stored with the third country or international organisation.

Such measures include ensuring that the rights of data subjects can be carried out and enforced and that effective legal remedies for data subjects are available. ***The appropriate safeguards can be provided without Supervisory Authority authorisation by: -***

- A legally binding and enforceable instrument between public authorities or bodies
- Binding corporate rules
- Standard data protection clauses adopted by the Commission

- Standard data protection clauses adopted by a Supervisory Authority and approved by the Commission
- An approved code of conduct together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regard data subjects' rights
- An approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regard data subjects' rights

With authorisation from the Supervisory Authority, the appropriate safeguards may also be provided for by: -

- Contractual clauses between JSL and the controller, processor or the recipient of the personal data in the third country or international organisation
- Provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights

JSL does not transfer personal data to any third country or international organisation without one or more of the above safeguards being in place or without the authorisation of the Supervisory Authority where applicable. We verify that any safeguards, adhere to the GDPR Principles, enforce the rights of the data subject and protect personal information in accordance with the Regulation.

Pursuant to Article 46, we ensure that any agreement, contract or binding corporate rules for transferring personal data to a third country or international organisation, are drafted in accordance with any Supervisory Authority and/or the Commission's specification for format and procedures (*where applicable*). ***As a minimum standard, we verify that the below are specified: -***

- The structure and contact details of the group engaged in the activity and of each of its members
- The data transfers or set of transfers, including: -
    - the categories of personal data
    - the type of processing and its purposes
    - the type of data subjects affected
- the identification of the third country or countries in question
- Their legally binding nature, both internally and externally
- The application of the general data protection principles, in particular: -
    - purpose limitation
    - data minimisation
    - limited storage periods
    - data quality
    - data protection by design and by default
    - legal basis for processing
    - processing of special categories of personal data
    - measures to ensure data security
    - the requirements in respect of onward transfers to bodies not bound by the binding

corporate rules

- The rights of data subjects regarding processing and the means to exercise those rights, including the right: -
    - not to be subject to decisions based solely on automated processing (*inc profiling*)
    - to lodge a complaint with the competent Supervisory Authority and before the competent courts of the Member States
    - to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules
- Our acceptance (*and that of any processor acting on our behalf*) of liability for any breaches of the binding corporate rules by the third country or international organisation to whom the data is being transferred (*with exemption from that liability, in whole or in part, only where we prove that we are not responsible for the event giving rise to the damage*)
- How the information on the binding corporate rules and the information disclosures (Articles 13/14) is provided to the data subjects *(with particular reference to the application of the GDPR Principles, the data subjects rights and breach liability*)
- The tasks of any Data Protection Officer and/or person(s) in charge of monitoring compliance with the binding corporate rules, as well as monitoring training and complaint-handling
- The complaint procedures
- The mechanisms within the group engaged in the activity, for ensuring the verification of compliance with the binding corporate rules, including: -
    - data protection audits
    - methods for ensuring corrective actions to protect the rights of the data subject
    - providing the Data Protection Officer and controlling board with such verification results
- The mechanisms for reporting and recording changes to the rules and reporting those changes to the Supervisory Authority
- The cooperation mechanism with the Supervisory Authority to ensure compliance by any member of the group, in particular by making available to the Supervisory Authority, the results of verifications of the measures referred to above
- The mechanisms for reporting to the competent Supervisory Authority any legal requirements to which a member of the group is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules
- The appropriate data protection training to personnel having permanent or regular access to personal data

5.3 TRANSFER EXCEPTIONS

JSL does not transfer any personal information to a third country or international organisation without an adequacy decision by the Commission or with Supervisory Authority authorisation and the appropriate safeguarding measures; unless one of the below conditions applies. ***The transfer is: -***

- made with the explicit consent of the data subject, after having been informed of the possible risks and the absence of an adequacy decision and appropriate safeguards
- necessary for the performance of a contract between the data subject and JSL or the implementation of pre-contractual measures taken at the data subject's request

- necessary for the conclusion or performance of a contract concluded in the interest of the data subject between JSL and another natural or legal person
- necessary for important reasons of public interest
- necessary for the establishment, exercise or defence of legal claims
- necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent
- made from a register which under UK or EU law is intended to provide information to the public (*and which is open to consultation by either the public in general or those able to show a legitimate interest in inspecting the register*). Transfer made under this exception must not involve the entire personal data or categories of the personal data in the register and if the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

Where a transfer is not valid under Article 45 or 46 and none of the above derogations apply, JSL complies with the Article 49 provision that a transfer can still be affected to a third country or an international organisation where all the below conditions apply. ***The transfer: -***

- cannot be made by a public authority in the exercise of its public powers
- is not repetitive
- concerns only a limited number of data subjects
- is necessary for the purposes of compelling legitimate interests pursued by JSL which are not overridden by the interests or rights and freedoms of the data subject
- JSL has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment, provided suitable safeguards with regard to the protection of personal data

Where the above transfer must take place for legal and/or compelling legitimate reasons, the Supervisory Authority is notified of the transfer and the safeguards in place, prior to it taking place. The data subject in such instances is provided with all information disclosures pursuant to Articles 13 and 14, as well as being informed of the transfer, the compelling legitimate interests pursued, and the safeguards utilised to affect the transfer.

6 RESPONSIBILITIES

The Data Protection Officer has overall responsibility for reviewing data that is to be transferred to a third country or international organisation and is tasked with the continued review of the Commissions adequacy decisions, along with Supervisory Authority communication and authorisations where applicable.

Any employees involved in the transfer of personal data as categorised in this policy, must adhere to the conditions of this document and the regulations laid out in Chapter 5 of the GDPR.

7 APPENDIX 1

When transferring personal data to a third country or international organisation, JSL adheres to the appropriate safeguards defined in Article 46 of the GDPR and will comply with any safeguards relied for each country.

7.1 STANDARD DATA PROTECTION CLAUSES

JSL in agreeing to this International Transfer Policy will rely on Standard Data Protection Clauses adopted by a Supervisory Authority.

7.2 CONTRACTUAL CLAUSES

JSL will accept and rely on any *Contractual Clauses* between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation that have been authorised by a Supervisory Authority.