

	Doc. Type <b>Policy</b>	Office <b>Amsterdam / London</b>	Initial Issue Date <b>25 May 2018</b>	Department <b>Legal</b>
Data Protection Policy applicable to CLSA (UK), CLSA Europe BV and CLSA BV		Version No.2	Last Revision Date <b>13 September 2018</b>	Owner <b>Marnix Mol, Amsterdam</b>
			Next Planned Review Date <b>September 2019</b>	Approver <b>Jaclyn Jhin, Hong Kong</b>

### Version Control

Version Number	Reason for change	Author	Date
1	Inclusion of CLSA Europe BV	Maxnix Mol	September 2018

### Approval History

Version Number	Approver	Date
1.1	Jaclyn Jhin	18.05.2018
1.2	Jaclyn Jhin	September 2018

**Contents**

1. Introduction.....3

2. Purpose .....3

3. Scope .....3

4. Personal Data.....3

5. Processing Personal Data.....3

6. The Data Protection Principles .....4

7. Consent.....5

8. Grounds for Processing Personal Data.....5

9. High Risk Processing Activities .....5

10. Fair Processing Information.....5

11. Third Party Service Providers.....6

12. Disclosure of Data .....7

13. International Transfers of Personal Data .....7

14. Retention and Disposal of Data .....7

15. Data Protection and Data Security .....8

16. Data Subject Rights .....8

17. Record Keeping .....9

18. Roles and Responsibilities .....9

## 1. Introduction

The General Data Protection Regulation (“GDPR”) in Europe and other related laws protecting personal data (the “Law”) regulate the way in which all personal data is held and processed. This policy describes how personal data must be collected, handled, stored, disclosed and otherwise “processed” to meet the Company<sup>1</sup>’s data protection standards and to comply with the Law. The meaning of the terms “personal data” and “processing” are provided in sections 3 and 4 below.

The Company regards the lawful and correct treatment of personal data as integral to our successful operations, and to maintain the confidence of the people we work with. The implementation and compliance by CLSA with GDPR are done by the Personal Data Committee (“PDC”)

## 2. Purpose

The purpose of this policy is to ensure that:

- everyone involved in the processing of personal data at the Company is fully aware of, and complies with, the requirements of the Law; and
- data subjects (a “data subject” being a person to whom personal data relates) are aware of their rights under the Law.

This policy should be read in conjunction with related policies and guidance as these provide more detailed guidance on correct handling of data.

## 3. Scope

All staff, consultants and other authorised third parties who have access to any personal data held by or on behalf of the Company must adhere to this policy.

## 4. Personal Data

In this policy, “personal data” includes any data which relates to a living individual resident in a country of the European Economic Area who can be identified from that data and other information which is in the possession of the Company or service providers. References to a “data subject” are to the individual whose data is being used.

Certain personal data is considered to be particularly sensitive and is subject to stricter rules regarding its processing. These categories of personal data are referred to as “sensitive personal data” and include any personal data relating to the racial or ethnic origin of the data subject; their political opinions; their religious beliefs; their physical or mental health condition; details of criminal offences and genetic and biometric data. The Company does not process sensitive personal data from its employees or clients.

The Company only holds personal data which is directly relevant to its dealings with a given data subject. That data will be held and processed in accordance with the Law and this policy.

## 5. Processing Personal Data

The word “process” includes any operation that is carried out in respect of personal data, including but not limited to collecting, storing, using, disclosing, transferring or deleting personal data.

Personal data collected by the Company is generally collected in order to:

- ensure that the Company can facilitate efficient transactions with, and perform its obligations and exercise its rights under contracts with, third parties including, but not limited to, its customers, partners, associates and affiliates;

---

<sup>1</sup> The term “Company” refers to either CLSA (UK) or CLSA BV.

- efficiently manage its employees, contractors, agents and consultants;
- efficiently and effectively manage its business; and
- meet all relevant obligations imposed by law.

An explanation of the lawful grounds for which personal data may be processed by the Company is provided in section 8 below.

Personal data may be disclosed within the Company and may be passed from one department to another in accordance with the data protection principles and this policy. Under no circumstances will personal data be passed to any department or any individual within the Company that does not reasonably require access to that personal data in order to achieve the purpose(s) for which it was collected and is being processed.

No department or individual within the Company may process personal data for any reason other than for the lawful purposes for which it was collected and is being processed.

## 6. The Data Protection Principles

Any person processing personal data must comply with the following core principles:

- **Lawfulness, fairness and transparency.** Personal data must be processed fairly, transparently and lawfully. You must not process an individual's personal data unless you have a lawful ground for doing so and you must inform a data subject of how and why you will process their personal data upon or before collecting it.
- **Purpose limitation.** Personal data must be processed only for specified and lawful purposes. Personal data must not be processed in any manner which is incompatible with those purposes.
- **Data minimisation.** The personal data that is processed must be adequate, relevant and limited to the minimum data necessary for the lawful purposes for which it is processed.
- **Accuracy.** Personal data must be accurate and, where appropriate, kept up-to-date. Any personal data which is incorrect must be rectified as soon as possible.
- **Data retention.** Personal data must be kept for no longer than is necessary in light of the lawful purpose(s) for which it is processed.
- **Rights of data subjects.** Personal data must be processed in accordance with the rights of data subjects. Data subjects will have the right to see copies of their personal data, to have inaccuracies corrected and to object to the processing of their personal data or to have their personal data deleted if it is no longer required by the Company for another important reason.
- **Security.** Personal data must be protected against unauthorised or unlawful processing, accidental loss, destruction or damage through appropriate technical and organisational measures.
- **International data transfers.** Personal data must not be transferred to a country or territory outside of the European Economic Area ("EEA") unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data or consent has been provided for such transfer.
- **Accountability.** The Company and its third party service providers are responsible for and must be able to demonstrate their compliance with this policy.

## 7. Consent

Personal data must only be processed if the purpose of the processing satisfies one of the lawful grounds permitted under the Law. There are various legitimate reasons for which personal data can be collected and used. One such reason is that the individual has consented to the use of their data. Other applicable reasons are described in section 8 below.

Within the Company we have legal grounds for the processing of the personal data of our employees and clients. However for the transfer of personal data to our offices abroad we may request our employees and clients for an explicit consent.

A record of consents should be retained by the Company to evidence that it has been authorised to carry out the processing of a data subject's personal data.

It is important to note that a data subject has the right to withdraw their consent at any time.

## 8. Grounds for Processing Personal Data

As noted above, consent is not the only basis on which personal data can be collected and used. There are other lawful grounds for processing personal data that the Company may be able to rely upon.

This section describes the lawful grounds for processing which are most likely to be relevant to the Company's processing activities. The legal grounds for processing personal data include where:

- the data subject has given their consent to the processing of their personal data. The requirements for obtaining a valid consent are explained in section 7 above;
- the processing is in the Company's legitimate interests and does not cause unwarranted prejudice to the data subject;
- the processing is necessary for the performance of a contract to which the data subject is a party, or for the taking of steps (at the request of the data subject) with a view to entering into a contract; or
- the processing is required by law.

## 9. High Risk Processing Activities

Wherever the processing of personal data is likely to result in a "high risk" to the data subject (for example, where it is particularly intrusive to a data subject's privacy), the Company will need to, before carrying out the processing activity, perform an assessment of the potential impact of the intended processing on the rights and freedoms of the data subject. The impact assessment should be conducted by the PDC.

## 10. Fair Processing Information

Any forms (whether paper-based or web-based) that gather data on an individual should contain a statement explaining what the information is to be used for and to whom it may be disclosed.

Regardless of how personal data is obtained, the data subject must be provided with certain information about the processing of their personal data by the Company. This information must be provided at or before the time at which the personal data is collected (or, if the personal data is obtained from a third party, within a reasonable time of obtaining the personal data or at the time of the first communication with the data subject, whichever is earlier).

The information provided to the data subject must include the following:

- the identity and contact details of the Company and the PDC;
- the categories of personal data collected in relation to the data subject;

- if the personal data is not obtained from the data subject, the source(s) of the personal data;
- the purpose(s) for which personal data will be processed, including the legal ground for the processing (see section 8 above). If the legal ground involves “legitimate interests”, a description of those legitimate interests must also be provided;
- if personal data is processed based on the data subject’s consent, an explanation of the data subject’s right to withdraw their consent at any time;
- the categories of personal data that may be disclosed to third parties and the reasons for these disclosures;
- if the data processing is a contractual requirement, whether the data subject is obliged to provide the personal data on that basis, and the possible consequences of a failure to provide the information;
- any intention to transfer the personal data outside the EEA and information the about the level of protection that will be afforded to the transferred data;
- information the about the existence of any automated decision making (for example, profiling) undertaken by the Company based on the personal data, including details of the logic involved and its impact on the data subject;
- the period for which the personal data will be retained, or the criteria that will be used to determine the retention period;
- a general description of the Company’s policies and practices with respect to protecting the confidentiality and security of personal data;
- the existence of the data subject’s rights; and
- any other information that is necessary to guarantee that the processing of the personal data is fair in the circumstances.

This information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language that will be easy for the data subject to understand.

If any of the information described above changes after it has been provided to the data subject, the data subject must be provided with an updated copy of the information.

## **11. Third Party Service Providers**

Where the Company instructs a third party to process personal data on behalf of the Company (referred to as a “data processor”), the third party must agree with the Company that it:

- provides details of the processing of personal data that they are being instructed to carry out;
- requires the third party to process the personal data only in accordance with the Company’s instructions;
- requires the third party to implement appropriate technical and organisational measures and controls to ensure the confidentiality and security of the personal data; and
- imposes any additional data processing obligations required by law.

The data processing agreements will be reviewed by the PDC. When contracting with a data processor, it is important that the Company conduct appropriate due diligence to ensure that the data processor is capable of complying with the requirements above.

## 12. Disclosure of Data

The Company must ensure that personal data is not disclosed to unauthorised third parties. All staff should exercise caution when asked to disclose any personal data to a third party. This section does not apply to data processors, which are addressed in section 11 above.

Personal data should not be disclosed orally or in writing to third parties without the consent of the data subject and approval from the PDC.

In some circumstances, the Law permits the disclosure of personal data without needing to obtain the prior consent of the data subject. Such disclosures might (depending on the circumstances) be permitted where this is necessary:

- to safeguard national security;
- for the prevention or detection of crime, in the substantial public interest, and where obtaining consent from the data subject would prejudice that purpose;
- for the administration of justice;
- to comply with applicable law; or
- to protect the vital interests of the data subject (this refers to life and death situations), but only where their consent cannot be obtained.

Requests for personal data from third parties must be supported by appropriate paperwork and any disclosures must be approved by the PDC.

## 13. International Transfers of Personal Data

Personal data must not be transferred outside the EEA unless the recipient country ensures an adequate level of protection for the rights and freedoms of data subjects. This requirement can be satisfied by:

- the recipient country having been subject to an “adequacy determination” by the European Commission (to date, only a handful of countries are subject to an adequacy determination, such as Canada and Israel);
- the entry into a data transfer agreement between the Company and the non-EEA recipient of the personal data which contains standard contractual clauses that have been approved by the European Commission; or
- consent have been provided by the data subjects for such transfers.

Before such a transfer takes place, you must first check with the PDC to determine whether the transfer is lawful.

## 14. Retention and Disposal of Data

Personal data must not be retained for longer than is necessary for the lawful purposes for which it is processed. To achieve this, each category of personal data processed by the Company must be subject to a retention period which can be justified by reference to those lawful grounds. Retention periods must be monitored and, upon their expiry, the relevant personal data must be deleted or anonymised.

For example, once an employee has left the Company, it will not be necessary to retain all the information held on them because much of this is only required to administer the employment relationship, such as bank details for salary payments. Some data will need to be kept for longer periods than others, for example where it is necessary to retain certain records in order for the Company to comply with its legal obligations.

Personal data must be disposed of securely in a way that protects the rights and privacy of data subjects and ensures the permanent erasure of the data (e.g. shredding, disposal as confidential waste, or secure electronic deletion). Hard drives of redundant PCs should be wiped clean before disposal.

## 15. Data Protection and Data Security

It is critical that the Company protects the personal data in its possession or control by applying appropriate technical and organisational security measures to protection the data.

In addition to the specific security policies that apply, all staff must comply with the following when processing and / or transmitting personal data:

- Personal data, whether held electronically or in paper form, must be kept securely at all times. The Company must ensure that measures are in place to prevent unauthorised or accidental access, use, disclosure, loss or damage when personal data is being processed. Technical measures, for example, include using encryption tools to protect personal data held in electronic form. Organisational measures, for example, include storing paper records containing personal data in locked cabinets.
- It is essential that if personal data is lost, damaged, compromised, misdirected or stolen, or otherwise processed in an unauthorised manner, that it is reported to the PDC.
- Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data in accordance with section 14 above.
- Personal data should not be disclosed except in accordance with sections 11 and 12 above.

## 16. Data Subject Rights

Data subjects are entitled to exercise certain rights in respect of their personal data. These rights include:

- the right to obtain information regarding the processing of their personal data and access to the personal data which the Company hold the about them;
- the right to receive a copy of any personal data which the Company processes the about them;
- the right to request that the Company rectify their personal data if it is inaccurate or incomplete;
- the right to request that the Company erase their personal data in certain circumstances. This may include (but is not limited to) circumstances in which:
  - it is no longer necessary for the Company to retain their personal data for the purposes for which we collected it; or
  - the Company are only entitled to process the data subject's personal data with their consent (i.e. because no other lawful ground for processing the personal data applies), and the data subject withdraws their consent; and



- the right to lodge a complaint with the data protection regulator, the Information Commissioner's Office, if the data subject thinks that any of their rights have been infringed by the Company.

Requests to exercise these rights should be sent to the PDC immediately upon receipt.

## 17. Record Keeping

Accurate and up to date records of the processing activities carried out by the Company must be maintained within the organisation. These records must include:

- details of the PDC;
- the purposes of the processing;
- the categories of data subject;
- the categories of recipients of personal data;
- the categories of transfers of personal data to countries outside the EEA;
- the envisaged time limits for erasure of the personal data (where possible); and
- a general description of the technical and organisational security measures adopted by the Company.

The PDC will keep a central record of the Company's processing activities and new processing activities or material changes to existing processing activities must be notified to the PDC.

## 18. Roles and Responsibilities

The Company board of directors are ultimately responsible for ensuring that the Company meets its legal obligations.

The PDC is responsible for:

- keeping the Company board updated the about data protection responsibilities, risks and issues;
- reviewing all data protection procedures and related policies;
- arranging data protection training and advice for employees;
- handling all data protection queries for employees;
- dealing with all requests from individuals to see the data the Company holds the about them (Subject Access Requests); and
- checking and approving any contracts or agreements with data processors.

The Head of Information Security is responsible for:

- defining security policies as well as recommending, reviewing and approving security designs; and
- evaluating at request any third party services the Company is considering using to store or process personal data (i.e. cloud services).

**19. Contact**

Contact point persons for queries on the policy are the members of the PDC, they can be contacted via [gdpr@cls.com](mailto:gdpr@cls.com)

**Appendix I – Supporting/Related attachment**

Identify any documents relevant to the development of the policy.

1. Employee Privacy Notice
2. Client Privacy Notice