CLSA Australia Pty Ltd

Data Protection Policy

Table of Contents

Data Protection Policy

1. Introduction

CLSA Australia Pty Ltd ('CLSA APL') is subject to the Australian Privacy Act 1988, Privacy Regulation 2013, Australian Privacy Principles and the Australian Notifiable Data Breaches scheme which all regulate the way individual's personal data is handled.

This Data Protection Policy explains how CLSA APL handles our client's personal data and measures we have in place to ensure CLSA APL can engage securely with our clients and relevant stakeholders.

2. Scope

All CSLA employees, contractors 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.

3. Personal Data

CLSA APL collects relevant data that we believe is essential to provide our financial services or products to our clients. Most of the information outlined in this Policy are subject to regulatory requirements, for example, CLSA APL must evidence we have confirmed the identify of our clients in accordance with the Australian Anti-Money Laundering and Counter Terrorism Financing Act ('AML/CFT Act').

3.1 Examples of Personal Data

In order for CLSA APL to provide financial services to its Wholesale Clients the following types of standard personal information may be collected from you:

- Name
- Date of birth
- Address
- Telephone number
- Email address
- Other contact or identification information

3.2 Examples of Sensitive Data

In certain limited situations CLSA APL may be required to collect from you sensitive information. Examples of sensitive information are outlined below:

- Information about an individual's health
- Criminal convictions

4. Collection of Personal Data

Authorised employees from CLSAP APL or any of our related entities within the CLSA Group are authorised to collect personal data.

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.

5. CLSA use and disclosure of Personal Data

Generally the CLSA Group collects uses and discloses Personal Data for the following purposes:

- Processing applications for account opening purposes
- Account maintenance and operational duties relating to your account(s)
- Processing of transactions
- Managing your relationship with CLSA
- Carrying out your instructions or responding to you
- Preventing, detecting and investigating any misconduct or unlawful activities
- Complying with all applicable laws, regulations, rules etc.
- Addressing or investigating an complaints
- Provision of financial services

6. How you can access your data

Should you wish to obtain access to your personal data and/or make corrections you may contact us in writing addressed to the Data Protection Officer (please refer to section 14 for contact details). The CLSA Group may charge an administrative fee for this service. In exceptional circumstances, we reserve the right to deny you access to your Personal Data and will provide an explanation accordingly.

7. Retention of Personal Data

Personal Data will be held for as long as it is necessary to fulfil the purpose for which is was collected or as required by applicable laws. The maximum retention period for Personal Data is seven years.

8. Disclosure, Sharing and Transfer of Personal Data Overseas

Subject to the provisions of applicable laws in each region the CLSA Group operates in, your personal data may be disclosed or transferred to or shared with or retained by the following:

- Related entity of the CLSA Group
- Any third party service provider
- Our professional agents (e.g. law firms, executing Brokers, Clearing Houses and Settlement agents)
- Any local or foreign government agency, regulatory authority who have jurisdiction over CLSA

To the extent that we may need to transfer personal data outside our jurisdiction, we shall do so in accordance with the Personal Data legislation of that jurisdiction.

9. Data Security

The CLSA Group has taken all reasonable steps to protect personal data in our possession or control by implementing appropriate security control arrangements to prevent unauthorised access, collection of, and usage of personal data we hold accordingly.

10. Consent

By interacting with CLSA and submitting information to us or signing up for any financial services for financial products offered by us you agree and consent to:

- CLSA collecting, using, disclosing and sharing your personal data
- Disclosing and sharing such personal data to the CLSA Group's authorised service providers and relevant third parties

If you do not wish for us to continue to use your Personal Data or the Personal Data provided by you to us for any of the Purposes at any time in the future, you must notify us in writing addressed to the Data Protection Officer to withdraw your consent (see section 14). Depending on the circumstances, your withdrawal of consent may result in CLSA's inability to provide you with the services and/or products that we have been offering to you, and consequently, may result in the termination of your relationship and/or accounts with us.

11. Updates to the Data Protection Policy

CLSA may from time to time update this Data Protection Policy to ensure that it is consistent with our future developments, industry trends and/or any changes in legal or regulatory requirements. Such changes will be posted on our web-site.

Your continued use of our service will be taken as acceptance of the updated Data Protection Policy.

12. Third Party Websites

Our Corporate web-site may contain links to other web-sites. Please note that we are not responsible for the privacy practices of such other web-sites and you are advised to read the Privacy Statement of each web-site you visit which may collect your personal data.

13. Complaints

If you have any concerns or issues that need to be escalated in relation to privacy or your personal information please contact our Data Protection Officer in writing. We will seek to address any concerns that you may have through our complaints handling procedures. If you wish to take the matter further you may refer to the Office of the Australian Commissioner ('OAIC') accordingly at www.oaic.gov.au

14. Contact details of Data Protection Officer

The contact details of our Data Protection Officer are:

Email: Compliance.Australia@clsa.com

Mail: The Data Protection Officer

CLSA Australia Pty Ltd

Level 35, Grosvenor Place

Sydney NSW 2000

15. ANNEXURE A – Notifiable Data Breaches ('NDB') Policy

In 2017 the Notifiable Data Breaches ('NDB') regime in Australia was established under Part IIIC of the *Privacy Act 1988* ('Privacy Act'). As such from 22 February 2018 the new Part IIIC will be implemented where data breaches must be reported. Under this scheme a data breach is known as an Eligible Data Breach.

15.1 NDB Overview

The NDB scheme outlines requirements for Australian entities such as CLSA APL in its response to data breaches. Should a data breach occur and is likely to result in 'serious harm' CLSA APL must notify the Office of the Australian Information Commissioner ('OAIC') within 72 hours.

15.2 What is an Eligible Data Breach?

An eligible data breach arises when the following three criteria are satisfied:

- ***Data Breach*** – this occurs when there is unauthorised access to or unauthorised disclosure of personal data, or a loss of personal data that CLSA APL holds.
- ***Serious Harm*** – the data breach is likely to result in serious harm to one or more individuals
- ***Remedial Action*** – CLSA APL has not been able to prevent the likely risk of serious harm with remedial action.

15.3 What is a Data Breach?

The first step to determine if an eligible data breach has occurred involves considering whether there has been a Data Breach being:

- Unauthorised access to; or
- Unauthorised disclosure of personal data, or a loss of personal data

The main categories of Data Breaches under the NDB scheme are described below:

Unauthorised access

This is where personal data that CLSA APL holds on your behalf has been accessed by someone who is not permitted to have access. This includes unauthorised access by an employee of the CLSA Group, or a Contractor as well as unauthorised access by an external third party (such as by hacking). The CLSA Group have specific I.T. Security teams and controls to monitor this.

Unauthorised disclosure

This occurs when CLSA APL, (whether intentionally or unintentionally) makes your personal data accessible or visible to others outside of the CLSA Group (e.g. an employee of CLSA APL accidentally publishes a confidential data file containing personal data of clients on the internet).

Loss of personal data

This refers to the accidental or inadvertent loss of your personal data held by CLSA APL. (E.g. an employee of CLSA APL leaves personal data, unsecured computer equipment, or portable storage devices containing our client's personal data on public transport).

15.4 Serious Harm

Whereas 'serious harm' is not defined in the Privacy Act in the context of a data breach the OAIC have described it as any of the following:

- *Serious physical, psychological, emotional, financial or reputational harm*

15.5 Types of Personal Data and Serious Harm

Some types of personal data may be more likely to cause an individual serious harm if compromised. Examples of the types of information that may increase the risk of serious harm if there is a data breach include:

- 'Sensitive information' such as details about an individual's health
- Documents commonly used for fraud (e.g. Medicare card, driver licence, passport details)
- Financial information

15.6 Reporting a Data Breach

If CLSA APL has reasonable grounds to believe it has experienced an eligible data breach, it must promptly notify affected persons and the OIAC about the breach by submitting an Eligible Data Breach Statement within 72 hours.

The statement must include the following information:

- The date, or date range of the unauthorised access or disclosure
- The date CLSA APL detected the data breach
- The circumstances of the data breach
- Who has obtained or is likely to have obtained access to the information
- Relevant information about the steps CLSA APL has taken to contain or remediate the personal data breach

15.7 The OAIC Form for lodging Statements to the Commissioner

The OAIC has an on-line form for entities to lodge eligible data breach statements under section 26WK of the Privacy Act. The form is located at:

https://forms.uat.business.gov.au/smartforms/servlet/SmartForm.html?formCode=OAIC-NDB