Date
January 2020

Personal Information Handling Policy

Document Author:	Group Compliance	
Approval Date / Version No:	January 2020	V1.3
Document Owner:	Head of Group Assurance	

Contents

1 Introduction

Within this document, Pro Global Holdings Ltd and its associated businesses are collectively referred to as the 'Company'. This document is part of the Data Protection Suite of polices and states the company position on the handling of personal information, whether it be client information or that relevant to Company staff.

The company retains much information and data, some of which relates to individuals which, when collated, can lead to identification of those individuals. The company has a duty to safeguard that Personal information, keep it secure and ensure it is only used for the purposes for which it was originally obtained.

1.1 Roles & Responsibilities

Role	Who	Responsibilities
Policy Owner	Head of Group Assurance	Annual review of the policy Provide assurance to the Pro Global Holdings Board that the policy is observed across the company
Implementation	Country Compliance Officer	Ensure implementation of, and adherence to, this policy within their territory
Security of stored data	Group Head of Information Technology	Ensure the implementation of approved Information Security policies and procedures

This policy is supported by the other policies within the suite of Data Protection Suite and by the Business Record Retention policy. Users should also be aware of the IT Acceptable Use Policy and Internet Acceptable Use Guidelines. Users must also be aware of the Information Security policies maintained on FORUM and in particular the Organisation of Information policy.

1.2 Applicability

The Policy is applicable Group-wide to all directors, employees, temporary workers, consultants, contractors, agents and subsidiaries acting for, or on behalf of, the Company or associated persons. Consult your country-specific Compliance Framework document for information on national laws, rules or standards or information from a national Regulator that may guide implementation of this policy.

Where local (territory) data protection legislation provides for more strenuous measures, then that local guidance will take precedence. Any additional client specific instruction regarding protection of their personal information must also be followed.

1.2.1 Exclusions

This policy has no exclusions, it is applicable to all Company staff as above. Any breach of this policy will constitute a serious disciplinary, contractual and potentially criminal matter for the individual concerned and may cause serious damage to the reputation and standing of the Company.

1.3 Definition

Personal information is that collected by the company from its clients and potential clients via the website, telephone calls, emails, letters or any other means. It is also applicable to the personal information held by the company regarding its own staff, past and present.

Personal data is that which is pertinent to an individual, not an organisation, and is any piece of information that when combined with one or more other pieces of information about the individual could lead to that person being identified.

The company classifies this data as either Personal or Sensitive Personal, but for this policy statement, reference to personal data shall also include sensitive personal data.

- Personal data - is any information including facts and opinions and any indication of intentions, which relates to a living individual who could then be identified from that information. This could include for example, name, address, contact details, date of birth, national Insurance number, job title, bank account details and salary information, etc. This also could refer to client or claimant details given a 'unique reference number' in one archive (i.e. card index or microfiche), that can be crossed matched to a separate index thereby enabling their identification.
- Sensitive personal data - relates to a person's racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health or condition, sexual life, criminal offences, legal proceedings and convictions. The company will collect this information on its' staff to satisfy its recruitment procedures and comply with legal and regulatory requirements. The company may also receive this type of information as part of its business activities (i.e. underwriting or claims handling etc.) but whether on staff or client, this data is likely to be of a 'private' nature and it should be protected with greater care than other personal data.

2 The Policy

The company will collect, maintain, retain and safeguard personal data only for the purposes for which it was originally collected and for which the individual gave their consent. If wider use is desired, the individual must be asked for and give their consent to the new use.

Personal information will only be available within the company and if requested, be shared with Government authorities and third parties involved in court activities and associated third parties as required.

The company will take appropriate technical, physical, legal and organisational measures consistent with the privacy and data security requirements to safeguard personal data. All reasonable steps will be taken to ensure that the personal information is reliable, complete and accurate. Personal information will be retained for the period necessary to fulfil the purposes outlined.

The company will adhere to the guidance provided by the appropriate body whenever personal data held by the company is required to be transmitted internationally. Personal data must not be sent to a country classified as having inadequate protection for such data. In these cases – or if in doubt - liaise with your country Compliance department for guidance.

A transfer of personal data to another country not cleared as having adequate data protection laws must not take place without the prior approval of the sending country's Compliance Officer.

Note: where the company processes personal data on behalf of a client, the act of processing data in accordance with the client instructions means the responsibility to the individual policy holders for use of the data, remains with the client.

2.1 Access rights

Individuals may have the right to access, correct or request deletion of their personal information. Any such, requests must be notified to Group Assurance (group.assurance@pro-global.com) for further information.

3 Additional Information

3.1 Queries

For queries regarding the Group policy, contact the Head of Group Assurance.

For queries regarding country implementation of this policy, contact the country Compliance Officer.

3.2 Document history

Version No	Description	Date of Exec Approval	Date of Implementation
V1.0	First authorised issue	December 2017	December 2017
V1.1	Annual Policy Review	January 2019	January 2019
V1.2	Amend footer to new Head Office address	N/R	April 2019
V1.3	Annual Policy Review	9th January 2020	January 2020

Note: Minor amendments to this policy may be released as V1.1, 1.2 etc. If there is a major change, complete review or the number of minor amendments becomes too large, the next version must be released e.g. V2.0