# Data Retention Policy

## Information Security

| Role | Name |
|---|---|
| Policy Owner | Head of IT Operations & Security |
| Executive Sponsor | Director of Technology |

## Version History

| Version | Date | Author | Description | Status |
|---|---|---|---|---|
| 0.1 | 2nd Jan 2023 | Nelson Abrunhosa | Initial policy draft | Draft Issue |
| 0.2 | 10th Jan 2023 | John Powell | Policy review | Draft Issue |
| 1.0 | 18th Jan 2023 | Suba Tomazi | Policy approval | Live Issue |
| | | | | |
| | | | | |

# Contents

## 1. Statement of Policy

Phaidon International Ltd (the "Company" or "Phaidon") takes its responsibilities for protecting the confidentiality, integrity, and availability of data in its possession, custody, or control seriously. The reputation of Phaidon as a world-class talent acquisition company requires that its Associates protect all confidential, non-public information — including Personal Data — Phaidon receives, creates, and/or transfers through the use of reasonable administrative, technical, and physical controls and safeguards ("Safeguards").

For the avoidance of doubt, this Policy applies in addition to (and not in substitution for) any data privacy or data protection or similar or related policies, procedures, or guidelines that any Phaidon worldwide business unit, subsidiary, or affiliate company may have in place (the "Regional Policies"). Phaidon intends to comply with applicable laws, regulations, rules, and contracts protecting the confidentiality, integrity, and availability of data in its possession, custody, or control. To the extent that any pertinent Regional Policies or relevant laws, regulations, rules, or contracts impose stricter requirements than this Policy, Phaidon intends to comply with such stricter requirements to the fullest extent possible.

## 2. Purpose

This Policy aims to define the Company's obligations and responsibilities in the handling and storage of data in relation to the Data Protection Act 2018 and General Data Protection Regulation as adopted into English Law (GDPR).

This policy has been created to ensure compliance with:

> *Principle 5 of the Data Protection Act 2018*
> *Personal data processed under any legal basis or purposes shall not be kept for longer than is necessary.*

## 3. Scope

Principle 5 of the General Data Protection Regulation as adopted into English Law (GDPR)

> *Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.*

## 4. Responsible party

The Director of Technology is responsible for the implementation, coordination, and maintenance of the Information Security Policy.

## 5. Violations

Any violation of this or any other policy shall subject the offender to disciplinary action up to and including termination. Please see the Associate Sourcebook for details regarding Phaidon's disciplinary process.

## 6. Updates

Updates to this policy will be announced to Associates via management updates, intranet updates or email announcements. The last date the policy was updated will be noted in the Revision History section.

## 7. Exceptions

Exceptions to this policy must be reviewed by the Director of Technology , Data Protection Officer and the Security Manager

## 8. Data Protection

The data protection arrangements are set out in the following company policies:

- Data Protection Policy
- GDPR Compliance Policy
- Information Security Policy
- Data Privacy Policy

## 9. Retention of Data

Phaidon International will only keep personal data in order to fulfil the purpose of processing or to meet any legal or contractual obligations.

Phaidon International is generally bound to data retention requirements specified with contractual clauses or data processing agreements.

Appendix 1 lists the retention periods for all company data assets

## 10. Compliance

The retention periods listed in Appendix 1 will be subject to internal audit, aligned with ISO 9001 & 27001 requirements and guidelines.

## Appendix 1 - Data Retention Schedule

| Data Asset | Retention Period |
|---|---|
| Candidate personal data | Held for as long as our interest is legitimate |
| Client Contact personal data | Held for as long as our interest is legitimate |
| Client confidential data | Up to 6 years from termination of relationship |
| Internal Hires personal data | Held indefinitely during employment and up to 3 years after employment ends |
| Candidate Sensitive Data (passports, social security numbers etc.) | Held for as long as there is a legal basis. Typically contractors and held only for duration of contract and up to 12 months from completion of contract |
| Supplier staff personal data | Up to 3 years from termination of relationship |
| | |
| | |