DATA RETENTION POLICY - THIS POLICY APPLIES TO THE FOLLOWING COMPANIES

OSPREY CLARKE LTD	OSPREY CLARKE INTERIM EXECUTIVES LLP	OSPREY CLARKE INTERNATIONAL AND EMERGING MARKETS LLP	PANDION RESEARCH LLP

1. INTRODUCTION

1. All Businesses named above are committed to protecting the personal information and privacy of the candidates we represent and the clients for whom we work.
2. Our legal obligations in respect of data retention depend on the particular nature of the personal data. Some types of personal data can and should be deleted within a relatively short timeframe, whilst others must be retained for a certain time either to comply with legal obligations or for some other legitimate reason.
3. Article 5(1)(e) of the General Data Protection Regulation (GDPR) also imposes an obligation on organisations that process personal data for a particular purpose, to keep that personal data for no longer than is necessary for the relevant purpose.
4. This Data Retention Policy (the Policy), together with any other documents referred to in it, sets out our arrangements for the retention and deletion of personal data that we collect from or about individuals (data subjects) It is intended to ensure that we adopt a consistent approach in respect of the main categories of personal data that we are likely to process, and that we can if necessary explain the rationale for our approach to the relevant authorities and the data subjects themselves.
5. This Policy applies to all copies of personal data that are held by us, or by our employees or contractors (staff), whether held on our own systems or on laptops, USB sticks or other storage devices in the possession of staff.
6. This Policy is the responsibility of Craig Marcham who is responsible for ensuring that it is enforced, and that the Policy itself is reviewed and updated at least once per year. 7. Infringements of this Policy

2. RETENTION PERIODS FOR PRINCIPAL CATEGORIES OF PERSONAL DATA

1. It is not practical or cost-effective for us to retain all personal data in perpetuity. Even if it were, it would not be permissible because of the GDPR principle that personal data should where possible be minimised. However, it is necessary to retain some data in order to protect our interests as a business, including for the purposes of meeting our own legal obligations with regard to record-keeping, where this is necessary in connection with potential litigation or for compliance with regulatory requirements, and otherwise for the purposes of good business and security practices.

2.The principal categories of personal data that we hold are outlined in the Appendix to this Policy. The Appendix also sets out, in respect of each category of personal data, how long we hold it for, and the rationale for that time limit. Where personal data is encrypted, we must also make arrangements for the encryption keys to be retained for the corresponding period, in order that the relevant data can be accessed if necessary

3. DISPOSAL ARRANGEMENTS

1. Once the retention period has elapsed for a given set of personal data, we will arrange for destruction of the data UNLESS we have received a request from the data subject to retain the relevant data for any reason (which requests must be referred to the person responsible for data protection in our company) or there is a compelling justification for continuing to hold the data (such as in connection with litigation).
2. Destruction of data will be carried out by one of the following means:

1. Records held in hard copy form must be destroyed by crosscut-shredding, pulped or burnt; and
2. Records held in electronic form must be permanently deleted (i.e. rendered non-recoverable by normal search processes) from our systems.
3. Destruction of the data may be outsourced to a reputable data destruction company, in which case we will require production of a written certificate of destruction.

APPENDIX

Principal categories of personal data and retention periods

Type of personal data	Description and/or examples	Retention Period	Notes
Candidate information	Name and contact details Education and qualifications Career history Current employer and job title Current compensation package Career objectives	6 years from the last contact with the relevant candidate, unless (a) the candidate has specifically consented to the data being retained for a further 12 months, and (b) that consent has been recorded in writing (including by email).	The GDPR requires that search firms observe a principle of data minimisation, which means not keeping personal data for longer than is necessary for the purposes for which we obtained it. In the case of candidates, the information that we hold about them potentially includes certain personal data of a sensitive nature (e.g. education, salary details), and we need to be particularly cautious about retaining this for longer than they might wish. There are no hard and fast rules about what the appropriate period should be, but if we have not had active communication with a candidate for a period of 6 years, and have no other reason for continuing to hold on to their details (e.g. because of possible litigation) then – for the sake of good business practice as much as legal compliance – we should check that the candidate is still content for us to continue to hold their personal data on file.
Client contact information	Name and contact details Current employer and job title	6 years from the last contact with the client contact, unless (a) the contact has specifically consented to the data being retained for a further 12 months, and (b) that consent has been recorded in writing, including by email.	The GDPR requires that search firms observe a principle of data minimisation, which means not keeping personal data for longer than is necessary for the purposes for which we obtained it. In the case of clients (e.g. HR departments and hiring managers), the information that we hold about them typically includes less personal data than is the case with candidates. Nevertheless, because of the more stringent requirements that GDPR imposes about retaining personal data just for marketing purposes, we need to be cautious that they are happy to remain on our database. There are no hard and fast rules about what the appropriate period should be, but if we have not had active communication with a client for a period of 6 years, and have no other reason for continuing to hold on to their details (e.g. because of possible litigation) then – for the sake of good business practice as much as legal compliance - we should as a matter of course check that the candidate is still content for us to continue to hold their personal data on file.

Employee and contractor information	Name and contact details Terms and conditions of employment/contractor agreement Employee files Payroll records (including salary, bonuses, overtime and expenses, and any other remuneration) Income tax and National Insurance returns Statutory Maternity Pay records Statutory Sick Pay records Accident records and reports	6 years from the end of employment (for employees) or from the end of engagement (for contractors).	The Limitation Act 1980 prescribes the time periods within which different types of action must be brought. The general rule applicable to actions in simple contract and tort is 6 years from the date on which the cause of action accrued. Our policy is accordingly to retain staff records until 6 years from the date of termination of employment, and then to dispose of them within a further 12 months as part of an annual cycle of data disposal. Records may be retained for longer periods if this is necessary in anticipation of ongoing or anticipated litigation.