PAMPLONA
CAPITAL MANAGEMENT

Pamplona Capital Management

Data Retention and Disposal Policy

June 2020

Version 2.0

PAMPLONA
CAPITAL MANAGEMENT

Version control

Version #	***Brief description of main changes***	***Changed by***	***Dated***
1.0	Original Version	Shoosmiths / Steve Gauci	October 2018
2.0	Annual Review	Kim Burnage / Steve Gauci	June 2020

PAMPLONA
CAPITAL MANAGEMENT

Contents

PAMPLONA
CAPITAL MANAGEMENT

1 Background, Purpose and Scope

1.1 Background

This Data Retention and Disposal Policy (the "Policy") applies to all employees of Pamplona Capital Management ("Pamplona") who come in to contact with personal data throughout their working day. In this Policy, we have summarized the key responsibilities the employee has, to ensure they comply with this and our other policies in relation to data protection (see also Pamplona Security Policy and Pamplona Data Protection Policy)

This Policy applies to Pamplona's (referred to as "we", "us", "our") employees, consultants, contractors, suppliers who have access to personal data and any business or other data which may or may not itself contain personal data.

Pamplona is made up of the following entities:

Legal Entity Name	Registration Number	Address	Country of Registration
Pamplona Capital Management LLP	OC 309813	25, Park Lane, London, W1K 1RA	United Kingdom
Pamplona Capital Advisors Ltd	5257246	25, Park Lane, London, W1K 1RA	United Kingdom
Pamplona PE Investments Malta Limited	C47993	5th Floor, Marina Business Centre, Abate Rigord Street, Ta' Xbiex, XBX 1127	Malta
Pamplona Capital Management (PE) S.L.	B87796132	c/ Marqués de la Ensenada, nº 2, 4ª Planta, 28004 – Madrid	Spain
Pamplona Capital Management (Monaco) SAM	17S07499	« Le Castellara » 9, avenue J.F. Kennedy 98000 Monaco	Monaco
Pamplona Capital Management LLC	5084410	667 Madison Ave 22nd Floor New York, NY 10065	United States

1.2 Why do we have a Document Retention and Disposal Policy?

Processing personal data is key to our day to day functions as a business. The General Data Protection Regulation (Regulation 2016/679) ("GDPR") requires us to only keep personal data for as long as is necessary, for the purposes for which it is intended and in accordance with a structured policy. This reflects the overarching principle of 'data minimization' under the GDPR, meaning that we should not be holding vast amounts of personal data where it is unnecessary.

If we keep too much personal data for too long, this can have a negative impact on the business:

- ✘ Customers complain when their information is out of date, inaccurate and / or used in error
- ✘ Risk of investigation by the Information Commissioner's Office and possible fines for the group for breaking the law (up to 4% of global group turnover)
- ✘ Risk we are unable to respond properly or quickly to a legal request for information from an individual
- ✘ Bad press and reputational damage associated with not treating personal data correctly

Accordingly, this Policy seeks to set out our principles and approach to retaining and ultimately disposing of personal data which we hold as an organization.

1.3 Data Retention Principles

To the end of achieving compliance with the GDPR, and to ensure consistency in how we retain and dispose of personal data as an organisation, we have a number of data retention principles which all Pamplona's staff must adhere to:

- All records and information have a designated owner, this may be an individual or a specific business area;
- It is necessary to ensure that records which may be required for audit, internal or regulatory purposes or potential litigation are not destroyed unless in accordance with the respective Annexes enclosed with this Policy;
- Except as above records should only be retained for legitimate business use and should not be kept longer than is necessary for the purpose it was collected;
- We have a Backup and IT Security Policy which applies to all data held within Pamplona; and
- All data is also encrypted.

1.4 Responsibilities

All employees must comply with this Policy, including its annexes. Failure to do so may cause us, and/or our employees and contract staff, to serious civil and/or criminal liability.

Managers are responsible for ensuring that the personal data that they and their team process is retained in accordance with this Policy. We must only keep what we need and permanently delete personal data that we do not need. Ask yourself: What is the purpose for holding the personal data, and how long have we said it will be retained for? If the data is no longer needed for this purpose then safely archive or securely delete the information.

To make sure you're doing the right thing, **you** should follow these practical steps:

Do:

- ✓ Only keep personal data for as long as the periods as set out in Annexes to this Policy and never keep something on a "just in case" basis.

- ✓ Regularly review what personal data you hold (e.g. in your emails, local or network folders or hard copy).

- ✓ Check whether any personal data is stored in shared folders. If so, check with your team whether you need it, and who should be permitted to have access to it (and regularly check this).

- ✓ Securely delete all copies of personal data that are no longer required.

- ✓ Securely destroy both paper and electronic records (use confidential waste bins and shred as appropriate).

Do not:

- ✗ Hold personal data in more than one place (e.g. in multiple folders in your team's shared drive).

- ✗ Store personal data in your email. Personal data sent by email should be extracted and saved in a secure shared folder or database. The original email should then be permanently deleted once its retention period has expired.

1.5 Governance

The person responsible for ensuring this Policy is followed is the Group Compliance Officer ('GCO'), Kevin O'Flaherty. Any questions about the operation of this Policy or any concerns that the Policy has not been followed should be referred to the GCO.

2 Types of documents or data subject to this Policy

This Policy refers specifically to 'personal data', however it is also concerned with retention of data more generally. We treat personal data differently and often to a higher standard to business or other data. For comprehensive information about all data we hold, and how long it is retained for, please consult the Annexes to this Policy.

It may not always be clear whether something constitutes personal data and a pragmatic approach should always be taken to determining this question. If you are at all unsure whether or not something constitutes personal data, you should contact your manager.

2.1 Personal Data

Information will constitute 'personal data' if it concerns an **identified or identifiable** living person. Personal data may be held within records, documents or confidential information relating to the organisation. For example, a business invoice may contain a name and signature (constituting personal data).

Documents or information which contain any 'special categories of personal data' about an individual or group of individuals must be treated with extra care – greater security and access rights limited.

For more information as to what constitutes 'personal data' and what our lawful business reasons for processing are please refer to our Data Protection Policy. If you are unsure whether to retain any personal data, contact your manager.

2.2 Business or Other Data

Much of the information we hold contains no information about identifiable individuals and thus does not constitute personal data. This means it falls outside of the GDPR regulations and does not need to be dealt with in the same way as personal data.

Examples of non-personal data are:

- Business to business contacts (save for director's names);
- Invoices (again people may be specifically named);
- Business performance data; and
- Accounts / Audit data.

These are subject to the retention period described in Annex B.

3 Storing, handling and archiving documents

If you need personal data for a business purpose, it is **your** responsibility to store it in the correct place and to regularly review who has access to it:

✓ Always store hard copy documents in locked filing cabinets – keep a clear desk	✗ Never leave hard copy documents on your desk, desk trays or unlocked pedestals
✓ Always save electronic data in the right shared drives and use the official pamplona drives. Details are given in Pamplona IT Security Policy.	✗ Never save electronic data on your local desktop or keep it in your emails or send it to your personal email

3.1 Electronic Records

Where documents and records are stored in any IT system or other electronic storage device, you must comply with our IT Security Policy.

Documents or files containing personal data or particularly sensitive business data (including attachments to emails) must never be stored on a personal laptop or mobile device in unencrypted form. All Pamplona provided laptops are encrypted.

3.2 Email records

Email is a vital tool to communicate with colleagues, suppliers and customers. However, you should remember that emails will often contain personal data or business records. It is important that such emails are treated as coming under this Policy and are stored or destroyed only in accordance with this Policy and its annexes.

4 Retention Periods

The Annexes included within this Policy set out the 'default' retention period for categories of personal data and business / other data. Default periods are calculated to protect us from potential exposure. In some cases documents will fall within an exemption to the default retention period where records should be kept for a longer or shorter period of time. These exemptions are also set out in the Annexes.

You should carry out a regular review of all documents and data that you hold or control against the Annexes and ensure that any applicable documents (all copies in all formats) are securely destroyed.

5 Destruction and Disposal

We prohibit the inappropriate destruction of any records, files, documents, samples and other forms of information. Therefore, this Policy is part of an organisation-wide system for the review, retention and destruction of records which we create or receive in the course of business.

The accidental or intentional destruction of these records during their specified retention periods could result in the following consequences for us and/or our employees.

- fines and penalties;
- disciplinary / regulatory action;
- legal claims;
- criminal liability; and/or
- loss of business amenity.

The relevant document owners are responsible for the continuing process of identifying the records and documents that have met their required retention period and supervising their destruction.

You should follow the guidelines below when disposing of data. There are certain circumstances where we may be legally compelled to dispose of data, such as: as the result of a court order; in response to a data subject exercising their rights; or in line with legislative requirements.

Records and documents that are subject to a "disposal hold" must not be destroyed until the GCO has confirmed they can be. See 6 below for further information.

5.1 Disposing of Paper Documents

When discarding paper records that contain personal data or business data, you must not place them in general waste paper or recycling bins. Instead, they should be disposed of in the confidential waste bins or by shredding.

5.2 Deleting and Archiving Electronic Documents

There is a significant difference between:

- deleting documents and data so they cannot be retrieved,
- archiving files or emails it in a structured, retrievable way; and
- leaving files or emails in an un-emptied electronic wastebasket such as a "recycle bin" (some e-mail programs store deleted items in a "deleted items" or "trash" folder).

Within Pamplona copies of all Pamplona emails are retained within Mimecast.

Where files are archived or sent to the recycle bin or “deleted items” folder, they will not be considered to have been deleted or disposed of for the purposes of this Policy. You should ensure that you empty both the “recycle bin” and the “deleted items” folder periodically

It should be noted that GDPR will still apply in respect of any personal data held in archived files or an electronic wastebasket, accordingly, so will this Policy.

It is recognized that it is not always practical to permanently delete data. In particular, where documents or data are ‘deleted’ from a PC, laptop or device they may still exist, in some form or another, within our IT systems.

Where any personal data cannot be deleted for practical reasons, it is acceptable to apply certain techniques or safeguards to put that personal data “beyond use”. This means that we:

- must not be able, or will not attempt, to use the personal data to inform any decision in respect of any individual or in a manner that affects the individual in any way;
- must not give any third party access to the personal data;
- all data that is held in archive/back up is held securely
- must commit to permanent deletion of the information if, or when, this becomes possible.

Provided all of the above safeguards are in place, personal data treated in this way:

- will not be considered ‘live’;
- will be considered “deleted” for the purpose of complying with the GDPR; and
- need not be searched in connection with any data subject rights requests.

We will make it clear to people what will happen to their personal data when we no longer need it (for example when their account closes). We will inform individuals whether their personal data will be deleted irretrievably or simply deactivated or archived.

Where we offer individuals the option to delete personal data uploaded by them, the deletion will be real (i.e. the content will not be recoverable in any way). It is bad practice to give a user the impression that a deletion is absolute, when in fact it is not.

5.3 Information held by Processors

Where suppliers or third parties hold data on our behalf and are asked to destroy these for a legitimate reason (such as expiry of a contract or withdrawal of consent), certificates of destruction should be requested as proof of destruction to support the audit trail of the records.

6 Disposal Holds

From time to time, the GCO may inform you, that our records are relevant to:

- current litigation or potential litigation (that is, a dispute that could result in litigation), government investigation;
- audit or other event; or
- other types of events, such as a merger or the replacement of our IT systems.

This exception is referred to as a "disposal hold" and replaces any previously or subsequently established destruction schedule for those records. In this event you must preserve and not delete, dispose, destroy or change those records, including e-mails, until you are informed that those records are no longer needed.

You must keep confidential the existence and circumstances of any disposal hold.

If you believe this exception may apply, or have any questions regarding whether it may possibly apply, please contact the GCO.

The GCO will consider whether any disposal hold extends to a supplier or third party, and will send a disposal hold notice as applicable.

Disposal holds should not be kept in place longer than necessary. Holds will be released immediately by the GCO when matters close and will be reviewed at least every 12 months to check they are still needed.

A sample Disposal Hold Notice is attached to this Policy at Annex D for use by the GCO.

PAMPLONA
CAPITAL MANAGEMENT

Annex A: Retention of Personal Data - UK

You should apply the standard retention period at the top of this table unless one of the exceptions below applies.

Customers

Document/Data Type	Period	Measured From
Paper Documents	1 year	Date on which data was originally received
Electronic Data/Documents	7 years	Date from which originally received or in the case of a contract date signed see below

Employees/Business Contacts

Document / Data type	Period	Measured From
Paper and Electronic Documents	7 years standard	Last day of employment/service contract
Any Contract signed as a deed	12 years from signature	Last day of contract
Signed Contracts	7 years from date of signature or 5 years from termination date reached.	Last day of contract
Employee Information		
Travel & Living Expenses	1 year	All measured from the last day of employment or service contract
Workplace grievance/complaints	1 year	
Eligibility to work documents and data	2 years	
Sensitive personal information (religious beliefs, union membership, convictions etc)	1 year	1st day of employment must be anonymised

PAMPLONA
CAPITAL MANAGEMENT

Annex B: Data Retention Schedule - Other Data - UK

Business

Document/Data Type	Period	Measured From
Paper Documents	1 year	Date on which data was originally received
Electronic Data/Documents	7 years	Date from which originally received or in the case of a contract date signed see below

PAMPLONA
CAPITAL MANAGEMENT

Annex C: Retention of Personal Data - Malta

Type of personal data	Retention period	Legal Basis for Retention
EMPLOYEE DATA Name Surname ID Card No. Address Telephone Number Mobile Number Email Date of Birth Gender Start Date Previous Work History Assessment and Performance Reviews Complaints Received Disciplinary and grievance information Recruitment Information (CV, Qualification Certificates) Pre-employment test results	- Duration of employment; and - 6 years post termination of employment	- processing is necessary for the performance of a contract to which the data subject is party including employment contract; - processing is necessary for compliance with a legal obligation to which the controller is subject; - establishment or defence of legal claims for which the prescriptive period for making a claim is 5 years from the date of termination of the contract. This covers both unfair dismissal actions any possible (subsequent) civil actions against the Company.
Social Security Number Social Security Contribution Bank Account Holder Name Bank Account Number Bank Name & Branch IBAN Number Compensation History Payroll Record	- 11 years	- processing is necessary for compliance with a legal obligation to which the controller is subject – Article 163, Companies Act; and/or - establishment or defence of legal claims in terms of employee national insurance contributions and payments, the prescriptive period for which could exceed 10 years - Article 122, Social Security Act -
Marital Status Next of Kin and Emergency Contact Info Copy of Driving License (where applicable)	- Duration of employment	- Erased shortly after termination of employment.

CCTV Footage, Entry and exit logs (security logs),	– Rolling 90 days	- Processing for security purpose only.
Anti-Money Laundering Documents (including passport copies, copies of utility bills and due diligence reports	– Duration of the business relationship – Six years after the termination of the business relationship	- Processing is necessary for compliance with the Anti-Money Laundering Act- Chapter 373 of the Laws of Malta
Records of company income and expenditure, profit and loss accounts, statements of assets and liabilities	– 10 years	- Processing is necessary for compliance with the Income Tax Management Act (Chapter 372 of the Laws of Malta)
Tax records on transactions	– 7 years from the end of the year to which they relate; **or** 7 yeards from the date when a tax return is provided of the Inland Revenue Commissioner receives a request for correction	- Processing is necessary for compliance with the Value Added Tax Act (Chapter 406 of the Laws of Malta)
Contracts with third parties	– Duration of the contract and 6 years after expiry of the contract	- This takes into account the prescriptive period for contractual claims under the Civil Code (Chapter 16 of the Laws of Malta)

PAMPLONA
CAPITAL MANAGEMENT

Annex D: Sample Disposal Hold Notice

Pamplona has [received notice of a claim against it in connection with [insert a general description of the claim[1]] (the "**Matter**").

We considers this Matter to be confidential and, unless otherwise permitted, you should not discuss, publish or disclose any information relating to this matter without permission from the GCO.

We are in the process of identifying all paper and electronic documents that may be relevant to the Matter. You have been identified as a person who has had involvement with [the contract relating to][2] this Matter, or may possess relevant documents or communications. We request your attention and assistance in preserving this relevant information for our use by the legal team and its advisors in dealing with the Matter as appropriate.

To comply with our legal obligations, we must make all reasonable efforts to preserve, or suspend from deletion, overwriting, modification, or other destruction of all relevant paper or electronic data in your possession, custody, or control that is relevant to this Matter.

As part of this process, you must preserve all documents or communications that may be relevant for the time period of [insert date range]. This notice applies to all [paper and electronic documents and communications][3]. If you are unsure about whether certain paper or electronic documents are relevant, you should preserve them. As used in this Notice, the terms "document", "data", and "information" are used in the broadest sense and apply not only to paper documents but also electronic documents or communications. All documents and information, in whatever form, that are relevant to this Matter must be retained and preserved.

Electronically stored information is an important and potentially irreplaceable source for information in relation to this Matter. Failure to retain these documents or communications, whether intentionally or accidentally or to ignore this notice may result in the company's inability to [prosecute its claims or defend itself in any litigation][4]. Failure to do so could also result in financial and legal penalties against the company that could negatively affect the outcome of this Matter. **You must take every reasonable step to preserve this information until further written notice.**

If you are aware of any colleagues, suppliers or third parties not listed on this notice that you believe may have additional and relevant information, such as those who may be under your supervision, direction, or control, please notify the GCO whose detail s are at the end of this

[1] Please insert a general description of the matter. This may be a claim against Pamplona or circumstances where Pamplona might have a legal claim against a third party. The matter might not have yet resulted in a claim, but there may be a credible threat or possibility of proceedings being brought by or against Pamplona. A disposal hold may also be applied in relation to a government or regulatory investigation, audit, or other types of events such as the merger of the client with another organization or the replacement of their information technology systems.
[2] Delete wording in square brackets if this is not a general contractual matter
[3] If necessary, expand the wording in square brackets to include a checklist of the types of documents or records that you are putting a hold on.
[4] This is relevant where the disposal hold is in relation to a claim. Please adjust the wording where the hold relates to a regulatory or corporate matter.

notice. Additionally, if you know of any other former employees who may have relevant materials, please forward their names to the GCO.

You must continue to preserve all paper and electronic documents or communications until you have received written notice that the disposal hold has been released.

If you have any questions about this notice or your responsibilities to comply with this notice, please contact the GCO. We may also follow up with you directly regarding the preservation or collection of your data in response to this disposal hold notice.

Please reply to the GCO to acknowledge that you have read and understood the preservation obligation stated in this disposal hold notice. Your attention and assistance with this notice is greatly appreciated.

Kevin O'Flaherty
Group Compliance Officer
Pamplona Capital Management