CASTLE CAPITAL
Financial Planning

Data Protection Policy

Summary / Purpose	This document outlines strict rules and procedures about the way in which personal data and sensitive personal data is collected, accessed, used and disclosed, by Castle Capital Financial Planning and all staff, in order to help ensure that we are compliant with the General Data Protection Regulation and Irish Data Protection Act 2018.
Developed By	Castle Capital Ltd and Castle Capital Financial Planning
Target Audience / User	*Castle Capital Financial Planning*
Date	*1st January 2020*

Circulation / Sign-Off List

Document Owner	Castle Capital Ltd & Castle Capital Financial Planning
Distribution List	Castle Capital Financial Planning Employees
Security / Confidentiality	Castle Capital Financial Planning Employees
Maintenance Cycle	**Twelve months** The policy may be reviewed between such intervals in the event of any legislative or other relevant developments
Document Sign-Off	Castle Capital Ltd
Document Sign-Off Date	1st January 2020
Post Sign-Off Changes to Doc	Castle Capital Ltd, 1st January 2020

Document History

Version	Date	Brief description of modification
1.0	*1st January 2020*	process document

CASTLE CAPITAL
Financial Planning

Table of Contents

APPENDICES

Background

All policies, guidelines and procedures of Castle Capital Financial Planning reflects Castle Capital Financial Planning's commitment to the protection of the rights and privacy of individuals (including customers, staff and others) whose personal information is held by Castle Capital Financial Planning. Castle Capital Financial Planning has put in place a range of systems and procedures, which it reviews on a regular basis, in order to protect these rights and to be fully compliant with the provisions of the General Data Protection Regulation and the Data Protection Act 2018.

In order to carry out its core functions, Castle Capital Financial Planning needs to collect and use personal data (information) about its customer, staff, and other individuals who come into contact with Castle Capital Financial Planning. Castle Capital Financial Planning needs to process such data for purposes that include the advice and administration of financial transactions, recruitment and payment of staff, compliance with statutory and regulatory obligations, etc.

Castle Capital Financial Planning is legally obliged to safeguard the privacy rights of individuals in relation to the processing of their personal information for such purposes. The General Data Protection Regulation and the Data Protection Act 2018 provide for this by conferring rights on individuals as well as responsibilities on those persons processing personal data. Personal data, both automated and manual is data relating to a living individual who is or can be identified, either from the data itself or from the data in conjunction with other information held by Castle Capital Financial Planning.

CASTLE CAPITAL
Financial Planning

Principles of Data Protection

Castle Capital Financial Planning undertakes to perform its responsibilities under the regulation in accordance with the following Data Protection Principles;

- **Obtain and process information fairly:**
  Castle Capital Financial Planning obtains and processes personal data fairly and in accordance with its statutory and other legal obligations.

- **Keep it only for one or more specified, explicit and lawful purposes / Use and disclosure only in ways compatible with these purposes;**
  Castle Capital Financial Planning keeps personal data for purposes that are specific, lawful and clearly stated. Personal data will only be processed in a manner compatible with these purposes. Castle Capital Financial Planning only uses and discloses personal data in circumstances that are necessary for the purposes of for which it collects and keeps the data.

- **Keep it safe and secure:**
  To ensure confidentiality Castle Capital Financial Planning takes appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of data and against accidental loss or destruction.

- **Keep it accurate, complete and up-to-date:**
  Castle Capital Financial Planning operates procedures that ensure high levels of data accuracy, completeness and consistency.

- **Ensure it is adequate, relevant and not excessive:**
  Personal data held by Castle Capital Financial Planning is adequate, relevant and not excessive in both the gathering of the information and in data retention terms.

- **Retain for no longer than is necessary:**
  Castle Capital Financial Planning has a policy on retention periods for personal data and a specific rationale for each chosen retention period.

CASTLE CAPITAL
Financial Planning

Roles & Responsibilities

Castle Capital Financial Planning has overall responsibility for ensuring compliance with Data Protection legislation as the Data Controller of personal data. However, all employees of Castle Capital Financial Planning who separately collect and / or control the content and use of personal data are individually responsible for compliance with the regulation and legislation.

The Compliance Officer provides support, assistance, advice and training to all staff to ensure that they are in a position to comply with the regulation and legislation. The Compliance Officer has responsibility for coordination and compliance relating to all Data Protection matters, including responding to general queries and Subject Access Request (SAR) requests received from Data Subjects relating to personal data as well as requests for assistance from firm employees involved in collecting, storing and processing personal information.

All staff should be aware that any received customer information should always be scanned to the customer file.

Procedures & Best Practice Guidelines

There are clear procedures in place at Castle Capital Financial Planning for the collection, processing and maintenance of personal information, required by Castle Capital Financial Planning to carry out its core functions. This Data Protection Procedures manual and Best Practice Guidelines set out these procedures in order to raise general awareness of the systems and procedures that are in place and to assist Castle Capital Financial Planning's employees to comply with Castle Capital Financial Planning's regulatory and legislative requirements under GDPR. Castle Capital Financial Planning's Data Protection Procedures and Best Practice Guidelines identify the areas of work in which Data Protection issues arise, and outline best practice in dealing with these issues.

Obtaining and processing personal data
Personal data is obtained fairly if the data subject is aware of the purpose for which Castle Capital Financial Planning is collecting the data, of the categories of person / organisations, to which the data may be disclosed / shared, of non-obligatory or optional answers in forms, of the right of access to the data and of the right of rectification of the data.

- Obtain personal data only when there is a clear purpose for so doing, obtain only whatever personal data is necessary for fulfilling that purpose and ensure data is used only for that purpose.
- The use of Castle Capital Financial Planning data processing facilities in capturing and storing personal data for non- business purposes must not take place.
- Inform data subjects of what personal information is held by Castle Capital Financial Planning, what it will be used for and to whom it may be disclosed / shared.
- Obtain explicit consent in writing for processing sensitive data and retain a copy of that consent. Consent cannot be inferred from non-response in the case of sensitive data.

Disclosing personal data

Personal data should only be disclosed in ways that are necessary or compatible with the purpose for which the data is kept. Special attention should be paid to the protection of sensitive personal data.

- Except where there is a statutory obligation to comply with a request for personal data, or where a data subject has already been made aware of disclosures, do not disclose to any third party any personal data without the consent of the data subject.
- Disclosure of personal data to a third party is not permitted unless there is a statutory obligation to disclose, or the information is released, to the Gardaí for example, for the prevention of crime and if informing the subject of the disclosure would prejudice the enquiries, or unless it is in the vital interest of the data subject.
- Personal data should only be disclosed to work colleagues where they have a legitimate interest in the data in order to fulfil administrative functions. Be satisfied of the need to disclose.
- Personal data should not be disclosed outside of the EU unless written consent has been obtained, unless disclosure is required for the performance of a contract to which the data subject is a party, or unless disclosure is necessary for the purpose of legal proceedings.

All staff should adopt a clean desk policy in line with best practices.

Securing personal data

Castle Capital Financial Planning must protect personal data from unauthorised access when in use and in storage or being destroyed and such data must be protected from inadvertent destruction, amendment or corruption.

- Personal electronic data should be subject to appropriate stringent controls, such as passwords, encryption, restricted access / access logs, backup, etc.
- Screens, printouts, documents, and files showing personal data should not be visible to unauthorised persons.
- Personal manual data must be held securely in locked cabinets, locked rooms or rooms with limited / controlled access.
- Subject to Castle Capital Financial Planning Data Retention Schedule, personal manual data should be destroyed by confidential shredding when the retention period has expired.
- When upgrading or changing PC, ensure the hard drive is cleaned by an appropriate / qualified IT staff member.
- Special care must be taken where laptops and PCs containing personal data are used outside Castle Capital Financial Planning.
- Special care must be taken to ensure the safety and security of any personal data held on mobile storage media.
- Health and work personal data can only be released following consultation with the relevant employee.
- Disclosing personal data to a Data Processor should be done only under a written contract specifying security rules to be followed.

Accuracy and completeness of personal data

Administrative procedures should include review and audit facilities so that personal data is accurate, complete and kept up-to-date.

Retention of personal data

Data should not be kept for longer than is necessary for the purpose for which it was collected. Data already collected for a specific purpose, should not be subject to further processing that is not compatible with the original purpose. All data held by Castle Capital Financial Planning should be stored and catalogued in accordance with the Data Retention Schedule and destroyed in accordance with that schedule and in compliance with regulatory and statutory obligations.

Disposal of personal data

Personal data should be disposed of when it is no longer needed for the effective functioning of Castle Capital Financial Planning and its employees. The method of disposal should be appropriate to the sensitivity of the data. Shredding is appropriate in the case of manual data and reformatting or overwriting in the case of electronic data. Particular care should be taken when PCs are transferred from one person to another or outside Castle Capital Financial Planning or are being disposed of.

Rights of the Individual

The Data Protection Acts provide for the right of access by a Data Subject to his or her personal information.
Data subjects must be made aware of how to gain access to their personal data. A Data Subject is entitled to be made aware of his or her right of access and to the means by which to access the data. A Data Subject is entitled to the following on written application within 30 days;

A copy of his or her personal data;

- the purpose of processing the data;
- the persons to whom Castle Capital Financial Planning discloses the data;
- an explanation of the logic used in any automated decision-making (where applicable);
- a copy of recorded opinions about him or her, (all staff should be conscious of this when making nay notes on a customer's file or sending internal communications which relate to the data subject)

The right of access is restricted where the data are:

- required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders, or assessing moneys due to the State;
- subject to legal professional privilege;
- kept only for statistical or research purposes and the results are not made available in a way that identifies data subjects;
- back-up data.

Provision of access to third parties

A Data Subject is entitled to access his or her own personal data only. The personal information of a Data Subject, including confirmation of attendance at Castle Capital Financial Planning or contact details, must not be disclosed to a third party, be they civil partner or spouse, potential employer, another employer, professional body, sponsor, etc., without the consent of the individual concerned.

An agreement may be made to forward a communication to a Data Subject on behalf of a third party, but no information should be disclosed about the Data Subject. In the case of research surveys where there is an agreement to forward documentation to Data Subjects, a notice should be included to the effect that no personal information has been released.

Limitations on the use of personal data for research / analysis

It should be noted that if research data is retained in personally identifiable format it may be subject to an access request from a data subject but should only be used were consent was freely given by the data subject.

Right of rectification or erasure

Data subjects have a right to have personal data rectified, or blocked from being processed or erased where the Data Controller has contravened the Act.
In order to comply with the above rights of access, rectification or erasure, ensure that personal data can be located and collated quickly and efficiently;

- Ensure personal data is in a format that is easy to locate and collate;
- Verify that the access request and the personal data released refer to the same individual;
- Know exactly what data is held on individuals, where and in some circumstances by whom;
- Hold personal data in a secure central location.

Responsibilities of Data Subjects

Castle Capital Financial Planning is dependent on Data Subjects themselves for maintaining the accuracy and currency of records held about them. The firm cannot be responsible for any inaccuracies resulting directly from the submission of such information by Data Subjects nor can it be accountable for any subsequent changes to such information unless notified. All Data Subjects have the right to review personal information, about themselves, recorded and stored by the firm and to have it amended if necessary. All Data Subjects (including staff and others) are entitled to be informed as to how their personal data can be kept up to date and accurate by Castle Capital Financial Planning.

All staff and other data subjects are responsible for;

- checking that any information that they provide to Castle Capital Financial Planning is accurate and up to date;
- informing Castle Capital Financial Planning of any changes of information, that they have provided,
- e.g. a change of address;
- checking / reviewing the information the firm sends out from time to time, giving details of information kept and processed, to ensure it remains accurate;
- informing Castle Capital Financial Planning of any errors or changes (the firm cannot be held responsible for any errors unless previously informed).

Where any such changes have been advised to the firm, these must be updated and corrected immediately or as soon as is reasonably possible.

CASTLE CAPITAL
Financial Planning

Data Access Request

Summary / Purpose	This document sets out the steps to follow if we receive a Data Access Request from a living individual, under the requirements of the General Data Protection Regulation 2018 and the Irish Data Protection Act 2018. It also advises how to record this request, who should send it and what we must provide to the data subject.
Developed By	*Castle Capital Ltd & Castle Capital Financial Planning*
Target Audience / User	*Castle Capital Financial Planning Employees*
Date	*1st January 2020*

Circulation / Sign-Off List

Document Owner	Castle Capital Ltd & Castle Capital Financial Planning
Distribution List	Castle Capital Financial Planning Employees
Security / Confidentiality	Castle Capital Financial Planning Employees
Maintenance Cycle	**Twelve months** The Policy may be reviewed between such intervals in the event of any legislative or other relevant developments.
Document Sign-Off	Castle Capital Ltd
Document Sign-Off Date	1st January 2020
Post Sign-Off Changes to Doc	Castle Capital Ltd, 1st January 2020

Document History

Version	Date	Brief description of modification
1.0	1st January 2020	process document

CASTLE CAPITAL
Financial Planning

Table of Contents

CASTLE CAPITAL
Financial Planning

Background

Under the requirements of the General Data Protection Regulation 2018 and the Irish Data Protection Act 2018, a living individual has the right to obtain a copy, clearly explained, of any information relating to them that we keep on computer or in a structured filing system. They have a right to be given:

- All personal information that Castle Capital Financial Planning holds about them
- A description of the categories of personal information we hold
- A description of the personal information
- The purpose for holding their personal information
- Where Castle Capital Financial Planning got their personal information
- Who it is passed to
- Confirmation if automatic processing was used

The living individual must write to us and ask for this information under the requirements of the General Data Protection Regulation 2018 and the Irish Data Protection Act 2018. If the customer's request for a copy of the information we hold is clearly set out in writing and quoting the Data Protection Act we can use this instruction, otherwise we should send them the Data Access Form to be completed and returned. Upon receipt of either a clearly worded letter or a completed Data Access Request Form we will arrange for a copy of all personal data to be issued to them. We must send the information within one month from receipt of the written request free of charge.

CASTLE CAPITAL
Financial Planning

Living Individuals' Rights

All living individuals have the right (with some exceptions):

- To enquire if we hold any personal information about them (See *Data Info Enquiry* procedure document)
- To request a copy of the personal information we hold about them

Only the living individual themselves can exercise this right in relation to their own personal data. The requirements of the General Data Protection Regulation 2018 and the Irish Data Protection Act 2018 do not apply to deceased persons or companies. Requests received should be carefully assessed to ensure they are categorised correctly. Where a subsequent clarification has been obtained from a data subject, this should be noted on file.

Enquiry Timescales

Time allowed:

- One month (from receipt of formal written request) to provide the living individual with a copy of their personal information held by us.

NOTE: We need to act quickly on these enquiries, as going through our records and sorting the information into a form readily understandable by the customer can take all of the allocated time. Day one is the date that we receive the request and we must respond within one month.

Exceptions to Right of Access

Individuals have a strong right of access to see their personal data. However, the General Data Protection Regulation 2018 and the Irish Data Protection Act 2018, sets out a small number of circumstances in which a person's right to see their records can be limited. You should refer to the Compliance Officer for any queries.

For example, in summary;

- If the information is kept for certain anti-fraud functions: but only in cases where allowing the right of access would be likely to impede any such functions

- If the information concerns an estimate of damages or compensation in respect of a claim against Castle Capital Financial Planning, where granting the right of access would be likely to harm the interests of Castle Capital Financial Planning.

- If the information would be subject to *Legal Professional Privilege* in court
- Therefore, if you come across documents labelled as '*Legally Privileged and Confidential*', please refer to the Compliance Officer to check if it is appropriate to send the document as part of the Data Access Request.

- If the information is kept only for the purpose of statistics or carrying out research, but only where the information is not disclosed to anyone else, and where the results of the statistical work or research are not made available in a form that identifies any of the individuals involved
- If the information is back-up data.

Note: It would be unreasonable to expect a firm to retrieve back-up copies of its personal information in responding to an access request. However, it should be noted that back-up data is not necessarily the same as old or archived data. Such archive data is subject to an individual right of access in the normal way.

Information about Other Individuals

The General Data Protection Regulation 2018 and the Irish Data Protection Act 2018, makes special provision for dealing with the personal data of another individual. A data controller is not obliged to comply with an access request if that would result in disclosing data about another individual, unless that other individual has consented to the disclosure. However, the data controller is obliged to disclose so much of the information as can be supplied without identifying the other individual, e.g. by omitting names or other identifying particulars.

Therefore, any third-party details and staff member names should be redacted.

Expressions of Opinion

Where the personal data consists of an expression of opinion about the Data Subject by another person, the Data Subject has a right to access that opinion except if that opinion was given in confidence. If the opinion was not given in confidence then the possible identification of the individual who gave it does not exempt it from access.
This is a very narrow exception. Therefore, as part of a Data Access Request, any communication available on file in respect of the data subject must be provided, unless it has been clearly given in confidence. Even where comments or emails on file are not very favourable, we still must provide them.

Therefore, all staff should be regularly reminded to be mindful that comments made in internal emails may be provided to the customer.

Disproportionate Effort

The General Data Protection Regulation 2018 and the Irish Data Protection Act 2018 provides that the obligation on a data controller to comply with a Data Access Request should normally be met by supplying a copy in permanent form, unless the supply of such a copy is not possible or would involve disproportionate effort.
Please note this does not exempt us from searching all records available, such as all systems where personal data may be stored, or call recordings. This just gives an exemption from providing a copy in permanent form.

Repeated Access Requests

If a Data Controller has complied with an access request he does not have to comply with an identical or similar request unless a reasonable interval has elapsed

CASTLE CAPITAL
Financial Planning

Recording Data Access Request - Process Steps

In Writing

Most Data Access Requests are received by the Principal or Compliance Officer, however if you come across a Data Access Request that has not been received correctly, or has not been recorded in the correct manner, please contact the Compliance Officer immediately. The below steps explain how to log a Data Access Request correctly.

- Review the received request and ensure this is a Customer Data Access Request
- If the request is not clear, contact the customer and ask, without prompting, what information they are looking for. The clarification obtained from the customer should be noted on file.
- If a satisfactory Data Access Request has been received the request should immediately be recorded on the Data Access Request spreadsheet and monitored for the timelines and review the complete file before sending this to the customer.
- The Data Access Request should be linked to the correct customer record and associated plans.
- The General Data Protection Regulation 2018 and the Irish Data Protection Act 2018 do not require us to acknowledge receipt of the request in writing. However, its good practice to send a Confirmation Letter to the customer so as to avoid repeat requests and to outline an expectation on the timeframe for a response. It's an opportunity to make the customer aware that we have one month, from the date the request was received, in which to provide the data.
- Prepare a file by reviewing all data systems and collating the Data Subjects information; a copy of **ALL** documentation relating to the customer / plan (s) to be printed and or retrieved from storage; compile the file along with an itemised letter that will be sent to the customer. (See Appendix B: ***Data Access Response Letter***)
- You must complete the response within month of the receipt date
- The spreadsheet should be reviewed daily to monitor the progress of any Data Access Requests noting when it was received and when the response was sent, and to report to Compliance Officer any instances which potentially could or are approaching the permitted timeframe as soon as possible.

Note: Sometimes the request for intormation is not a formal Data Access Reqeust; a customer could subsequently clarify that they are not seeking a full Data Access Request but only specific documents. Any request for information that is being sent but is not being treated as a formal Data Access Request should be saved to the worksheet called 'Non-DAR'. This is to help the Compliance Officer monitor the work and the progress of requests for information. Such requests should be handled by the agreet staff member (typically the Principal or Compliance Officer but should not take priority over Data Access Request.

CASTLE CAPITAL
Financial Planning

By Telephone

Most Data Access Requests are received in writing, however if you receive a request for data under the General Data Protection Regulation 2018 and the Irish Data Protection Act 2018, over the telephone you should;

- In line with normal procedures verify identity of enquirer (use relevant combination of e.g. First Name, Surname, Plan number, Date of Birth, plan details etc.), to establish the caller's identity.
- Keep in mind that only the individuals themselves can exercise their rights under the General Data Protection Regulation 2018 and the Irish Data Protection Act 2018, in relation to their own personal data. Exception can be made if a solicitor is making a request on behalf of the customer and a signed authorisation from the customer has been provided. Also, legal guardians can make a request for information on behalf of a child. (The Acts do not apply to deceased persons or companies.)
- If the request is not clear, the customer should be asked what information they are looking for. Please do not lead the customer to a Data Access Request if this is not what they intend, i.e. in order to determine whether the request is a Data Access Request, the customer should specify without prompting that they wish to obtain a copy of **ALL** of their personal data held. This clarification should be recorded on file.
- If the customer is only looking for a specific piece of information, such as a copy of a letter or a telephone call, this should be treated as a normal administrative request.
- If the customer clearly wishes to make a Data Access Request, the following steps should be followed;

    - Send the Data Access Request form to the customer or advise the customer they can send in a signed written request to the Principal or Compliance Officer at Castle Capital Financial Planning's address.
    - Customers should be advised that a Data Access Request is an individual request and relates to their personal data only. If there are multiple parties to the contract,
    - e.g. joint lives assured and both wish to receive a copy of their personal data, separate, individual Data Access Requests will need to be submitted in writing from each customer.
    - Customers should also be made aware that we have up to one month in which to respond to a Data Access Request, however where possible we will respond sooner.

To view a copy of the Data Access Request Form, see Appendix A

CASTLE CAPITAL
Financial Planning

Additional Procedure Notes

Searches

Staff must make every effort to trace all data relating to the customers' plans (unless only specific plan numbers are quoted in the request) including paper file(s), copies of all letters, documents, data on any other systems and telephone calls. Systems and sections that should be reviewed for personal information are as follows;

- Paper Files
- Computer Files
- Telephone Records

Financial Review

Note: A Data Access Request also includes any personal information linked to a Financial Review, regardless of whether the enquirer has ever set up a plan.

Terms Explained

We should check all documents being sent for any codes, terms or abbreviations that the customer may not be familiar with. If there are any we should include an explanation of these, in the form of a *Glossary of Terms*, to be included separately but as part of the response being sent.

Review of File

1. A copy of the redacted file is not kept. But it is important that a comprehensive itemised list is included in the response letter as proof of what information was sent to the customer. A copy of the response letter with an itemised list of what is being sent should be saved for future reference. **See Appendix B**: *Data Access Response Letter*.
2. The Data Access Request spreadsheet will be updated to confirm when the data has been sent, within the appropriate timeframe and to whom.
3. Each month a copy of the Data Access Request spreadsheet is sent to the Principal to make them aware of the number of data access requests, identify any trends and to show that all requests have been processed within the required timeframes.
4. Failure to process a Data Access Request within the prescribed timeframe is a ***breach*** of the Data Protection Legislation and the customer has the right to complain about this to the Data Protection Commissioner. The Compliance Officer should be notified about any delays which could potentially fall outside the prescribed timeframe, with an explanation as to why the request was not actioned within the prescribed timeframe and when the information is expect to be sent.

CASTLE CAPITAL
Financial Planning

Points to note

- A Data Access Request can only be made by a living individual.
- A Data Access Request can only be requested by the data subject themselves. Third parties are not entitled to access information about the customer without their express written permission. The default practice should be to provide any information requested by a 3rd party to the client directly, so that the client can forward it to the 3rd party themselves.
- Exceptions can be made if it is proven that the person requesting the data has approval from the data subject and it is clear that they are acting on their behalf, e.g. solicitor or parent of minor.
- Government bodies and other regulatory agencies do not have the right to access a customer's data without their permission. However, if you receive a request for information from a law enforcement authority, such as the Criminal Assets Bureau, under the Data Protection Acts, please let the Compliance Officer know immediately.

Please see below:

Disclosure of personal data in certain cases

Any restrictions in this Act on the [processing] of personal data do not apply if the [processing] is—

a. in the opinion of a member of the Garda Síochána not below the rank of Chief Superintendent or an officer of the Permanent Defence Force who holds an army rank not below that of Colonel and is designated by the Minister for Defence under this paragraph, required for the purpose of safeguarding the security of the State,

b. required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders or assessing or collecting any tax, duty or other moneys owed or payable to the State, a local authority or a health board, in any case in which the application of those restrictions would be likely to prejudice any of the matters aforesaid

- We can comply with a request for information from the Central Bank or Pension Authority. Please contact the Compliance Officer if you receive request from Central Bank or Pensions Authority.

- If a customer requests details about what personal information we have on file we should try and enquire if they are seeking a particular piece of information rather than a full data access request. If they only want a copy of outgoing letters or a specific piece of information, and it is not a Data Access Request.

- If we are sending emails/work documents, both internal and external, we should redact staff members and other third parties' names, contact details and any other personal information.

- We should check all documents being sent for any codes, terms or abbreviations that the customer may not be familiar with. If there are any we should include an explanation of these, to be included as part of the response being sent.

Letters

When responding to a Data Access Request we must ensure that we provide all information as required under the General Data Protection Regulation 2018 and the Irish Data Protection Act 2018. Therefore, we should use the letters and amend them as needed for each response, depending on what data we hold for the customer, and how it was obtained and used.

Appendix A: Data Access Request Form
Appendix B: Data Access Response Letter
Appendix G: Data Access Request Recording Grid

Data Info Enquiry

Summary / Purpose	This document sets out the steps to follow if a query is received in writing from a living individual, to find out if we hold information about them under the General Data Protection Regulation 2018 and the Irish Data Protection Act 2018. Note: they do not need to refer to this specific section of the Act. This document also advises how to record the request, who should send it and what we must provide to the data subject.
Developed By	Castle Capital Ltd & Castle Capital Financial Planning
Target Audience / User	Castle Capital Financial Planning Employees
Date	*1st January 2020*

Circulation / Sign-Off List	
Document Owner	Castle Capital Ltd & Castle Capital Financial Planning
Distribution List	Castle Capital Financial Planning Employees
Security / Confidentiality	Castle Capital Financial Planning Employees
Maintenance Cycle	Twelve months The Policy may be reviewed between such intervals in the event of any legislative or other relevant developments.
Document Sign-Off	Castle Capital Ltd
Document Sign-Off Date	1st January 2020
Post Sign-Off Changes to Doc	Jonathan McDonnell 01 January 2020

Document History		
Version	**Date**	**Brief description of modification**
1.0	*1st January 2020*	process document

CASTLE CAPITAL
Financial Planning

Table of Contents

Appendix C: Data Enquiry Response Letter

CASTLE CAPITAL
Financial Planning

Background

Under the General Data Protection Regulation 2018 and the Irish Data Protection Act 2018, an individual has the right to find out, free of charge, if we hold personal information about them. They also have a right to be given;

- a brief description of the information
- the purpose for holding their information
- to whom it is passed

The data subject must make this request in writing. We must send the information within 21 calendar days from receipt of the written request.

CASTLE CAPITAL
Financial Planning

Living Individuals' Rights

All living individuals have the right (with some exceptions) to;

- enquire if we hold any information about them
- request a copy of the information we hold about them (See Section - Data Access Request procedure document)

Only the living individual themselves can exercise this right in relation to their own personal data. The General Data Protection Regulation 2018 and the Irish Data Protection Act 2018 do not apply to deceased persons or companies. Requests received should be carefully assessed to ensure they are categorised correctly. Where a subsequent clarification has been sought and obtained from a data subject, this should be noted on file.

Enquiry Timescales

An individual should be informed in writing, not more than 21 calendar days from the date the request was received, as to whether we hold personal information on computer or not. The response should only outline;

- a brief description of the information
- the purpose for holding their information
- to whom it is passed

NOTE: It's important to act quickly on these enquiries, as going through all records and locating the information can take all of the allocated time. Day one is the date that the request is received.

Recording Data Info Enquiries- Process Steps

Most Data Info Enquiries are received by the Principal or Compliance Officer, however if you come across a Data Info Enquiry that has not been received correctly, or has not been recorded in the correct manner, please contact the Compliance Officer immediately. The below steps explain how to log a Data Info Enquiry correctly. All requests should be recorded on the Data Access Requests Spreadsheet under the tab 'Data Info Enquiry'. Once a request is received it should be added to the spreadsheet without delay. The spreadsheet should be used daily to monitor the progress of the request and when it was sent, and to report to the Principal.

CASTLE CAPITAL
Financial Planning

Process & Procedure Steps

Mostly such requests are received in writing. For all Data Info Enquiry Requests received in writing, record it to the correct tab on the Data Access Request Spreadsheet and notify the Compliance Officer immediately so that they can begin preparing and send a response letter, and complete and close the request on the spreadsheet.

In Writing

- The Compliance Officer will review the request and ensure that the customer has made a clear enquiry about the data (if any) that we hold under the Data Protection Act.

  Note: customer does not need to specify their intention under the Acts.

- If the request is not clear, the Compliance Officer will contact the customer and ask what information they are looking for, and explain what they need to do. The clarification obtained from the customer should be noted on file. If a satisfactory request has been received the Compliance Officer will ensure the request is recorded on the Data Access Request Spreadsheet under the correct tab and will monitor the timelines, prepare and send the response to the customer.
- The Data Protection Act does not require Castle Capital Financial Planning to acknowledge receipt of the request in writing. Best practice is to send an acknowledgement letter, confirming receipt of the request and to make the individual aware that we have 21 calendar days, from the date the request was received, in which to provide the full response.
- The Compliance Officer will arrange for **ALL** systems to be checked for any personal information that we may potentially hold so as to accurately describe this to the individual along with details outlining the purpose for holding the personal data and to whom it is passed.

By Telephone

- If a request to establish if we hold data is received by telephone;

- In line with Castle Capital Financial Planning DP procedures, verify identity of caller (use relevant combination of e.g. First Name, Surname, Plan number, Date of Birth, plan details etc.)

- If it can be confirmed, whist on the call, that Castle Capital Financial Planning holds no data for the individual, then staff can confirm that no information is held, during the telephone call.

- If the staff member taking the call believes that Castle Capital Financial Planning does hold some information, then tell the caller that, if they are making an enquiry under the Data Protection Act, i.e. enquiring if we hold data about them and they want a description of this data and the purpose of holding it, they must submit the request in writing in order to receive a formal written response.

Note: Its good practice to make the caller aware that we have up to 21 calendar days in which to respond to their query, however where possible we will respond sooner

Additional Procedure Notes

Searches

Staff must make every effort to trace all data relating to the customer on all systems, including paper file(s). Systems and sections that should be reviewed for personal information under a Data Info Enquiry Request are as follows;

- Paper Files
- Computer Files
- Telephone Records

Financial Review

Note: A Data Info Enquiry also includes any personal information linked to a Financial Review, regardless of whether the enquirer has ever set up a plan.

Review of file

- It is the responsibility of the Compliance Officer to ensure they have located all the personal data and suitably prepared the response to be sent to the data subject.
- A copy of the response letter must be saved to the appropriate folder.
- The *Data Info Enquiry Response Letter* in Appendix C should be used and amended as appropriate. The Data Access Request spreadsheet will be updated to confirm when the response has been sent and to whom.
- Each month a copy of the Data Access Request spreadsheet is reviewed with the Principal, to make them aware of the number of requests received and to demonstrate that all requests have processed these within the prescribed timeframes.
- Failure to process a Data info Enquiry Request within the prescribed timeframes is a breach of the Data Protection Legislation and the Individual has the right to complain about this to the Data Protection Commissioner. The Compliance Officer will notify the Principal about any potential delays, and advise why the data enquiry request was not completed on time and outline when this information is expected to be sent.

Points to Note

- Requests to establish if we hold data *only* apply to living individuals.
- A Data Info Enquiry can only be requested by the data subject themselves. Third parties are not entitled to access information about the customer without their express written permission. The default practice should be to provide any information requested by a 3rd party to the client directly, so that the client can forward it to the 3rd party themselves.
- Exceptions can be made if it is proven that the person making the query has approval from the data subject and it is clear that they are acting on their behalf, e.g. solicitor or parent of minor.
- Government bodies and other regulatory agencies do not have the right to access a customer's data without their permission. However, if you receive a request for information from a law enforcement authority, such as the Criminal Assets Bureau, under the Data Protection Act, please let the Compliance Officer know immediately.

- We can comply with a request for information from the Central Bank or Pension Authority. Please contact Compliance if you receive request from Central Bank or Pensions Authority.
- Any contact made with the customer about their enquiry must be recorded on the file as an Outgoing call, letter or email as appropriate.

Letters

When responding to a Data Enquiry we must ensure that we provide all information as required under the Data Protection Act, therefore the letter in Appendix C should be used and amended as required for each individual response, relative to what data we hold for the living individual.

Appendix C: Data Info Enquiry Response Letter

CASTLE CAPITAL
Financial Planning

Data Incidents & Breaches Process

Summary / Purpose	This document sets out the steps that should be followed if a Data Protection Incident is identified.
Developed By	Castle Capital Ltd & Castle Capital Financial Planning
Target Audience / User	Castle Capital Financial Planning Employees
Date	1st January 2020

Circulation / Sign-Off List	
Document Owner	Castle Capital Ltd & Castle Capital Financial Planning
Distribution List	Castle Capital Financial Planning Employees
Security / Confidentiality	Castle Capital Financial Planning Employees
Maintenance Cycle	**Twelve Months** The Policy may be reviewed between such intervals in the event of any legislative or other relevant developments.
Document Sign-Off	Castle Capital Ltd
Document Sign-Off Date	1st January 2020
Post Sign-Off Changes to Doc	Jonathan McDonnell 01 January 2020

Document History		
Version	**Date**	**Brief description of modification**
1.0	1st January 2020	process document

CASTLE CAPITAL
Financial Planning

Table of Contents

Appendix F: Notification of Data Breach Form

CASTLE CAPITAL
Financial Planning

Background

Data protection is safeguarding the privacy rights of living individuals in relation to the processing of personal data. The General Data Protection Regulation 2018 and the Irish Data Protection Act 2018 give rights to individuals (data subjects) and responsibilities to data controllers and processors. The rules are summarised as follows;

- Lawful, fair and transparent processing of personal data
- Limit to the purpose for which personal data is freely given
- Process personal data with integrity and confidentiality and keep it secure
- Retain personal data for no longer than is necessary
- Keep personal date accurate, complete and up to date
- Collect no more personal data than is necessary, relevant and not excessive

It is important that at all times we ensure that customers' data is kept secure and safe and is not put at risk. If we make a mistake, or suspect that a mistake has been made, and customers' data has been put at risk then this must be reported to the Compliance Officer. The Compliance Officer will report all incidents to the Principal each day. The Compliance Officer will review the incident and confirm to the Principal if a breach or non-breach has occurred and how to proceed.

The Compliance Officer will assist in the resolution of the problem by correcting the data, notifying the affected parties, making efforts to retrieve any data that was disclosed and suggesting measures to prevent this from happening again.

Please note a customer does not have to complain in order for a staff member to report a data protection incident to the Compliance Officer.

CASTLE CAPITAL
Financial Planning

Life cycle of Data Protection Incident

This is a general overview of the life cycle of a potential data protection incident.

- Issue is identified / notified and reported to the Compliance Officer
- The incident is set up on the Data Protection Incident Spreadsheet by whichever staff member discovers or is notified of the incident OR if not already done by the notifying staff member, the Compliance Officer will record details of the incident on the Data Protection Incident Spreadsheet
- The Compliance Officer will review each incident and confirm if it should be reported as a *breach* or *non-breach* and determine on how to proceed.
- The Compliance Officer will update details of the incident to the Principal.
- If no error has occurred and no complaint was raised the case can be withdrawn and marked as *No breach* on the Data Protection Incident Spreadsheet
    - The case can be referred back to the relevant staff member to resolve any outstanding issues / requirements or treat as a normal admin request in line with normal procedure.
- If an error has occurred or a complaint was raised the Compliance Officer will record the incident and take the necessary steps to investigate the incident to identify how the error occurred, notify the affected parties, secure the data and identify any Corrective and Preventative Actions
- If necessary the case may need to be reviewed with the Principal if it's a complex case or if a large number of customers were affected.
- Once all issues have been resolved a Data Protection Breach Notification Form will be completed, signed off by the Principal and saved to the relevant folder.
- The Data Protection Incident Spreadsheet should be updated to confirm the incident has been resolved, completed and closed.

Note: this is a general overview of the typical steps required to resolve most data protection incidents. However due to the varying nature of the issues that can occur, these steps can vary from case to case.

Reporting

Any incidents where customers' or employees' personal information has been put at risk of unauthorised disclosure, loss, destruction or alteration must be investigated. Where Castle Capital Financial Planning becomes aware of a data security breach or suspects a breach may have occurred this must be reported immediately to the Compliance Officer.

When reporting the incident ideally the notifying staff member should set out what plans were affected, what data was put at risk, how they identified the affected plans and any other important factors. Upon receipt of the data incident notice the Compliance Officer will be responsible for handling the incident in line with the Data Security Breach Code of Practice and Castle Capital Financial Planning Complaint Processes and Procedures.

CASTLE CAPITAL
Financial Planning

Note: it is possible that the exact details of what information has been disclosed and how this happened may not be fully available until a complete investigation has bee be conducted; however, this should not delay making the notification

Reporting incidents to Data Protection Commissioner

The Data Protection Commissioner (DPC) introduced a Code of Practice setting out the reporting obligations of a data controllers in the event of a security breach. This Code addresses situations where personal data has been put at risk of unauthorised disclosure, loss, destruction or alteration. Any incident which has put personal data at risk should be reported to the DPC within 72 hrs of the data controller becoming aware of it.

There are some limited exceptions to this where:

a) It affects fewer than 100 data subjects; AND
b) The full facts of the incident have been reported without delay to those affected; AND
c) The breach does not involve sensitive personal data or personal data of a financial nature; OR
d) if the personal data was protected by technological measures (such as encryption) to such an extent that it would be unintelligible to any person who is not authorised to access it, then the data controller may decide that there is no risk to the personal data and so no notification to the data subject is necessary.

The Compliance Officer is responsible for reviewing the initial report and deciding if they need to make an onward report to the Data Protection Commissioner.

To assist he Compliance Officer in their review of the case and ensuring that all incidents are treated as prescribed by the Data Protection Commissioner's guidelines, the initial report to the Compliance Officer (where possible) should indicate the proposed corrective action, that will be taken, and depending on the nature of the incident and what potential steps can be taken to resolve it as quickly as possible.

The Compliance Officer may request additional information, from the notifying staff member, to help determine the extent of the incident and if other customers could be affected for the purpose of reporting to the Data Protection Commissioner.

When the Compliance Officer has completed their review of the case they will determine if the case should be reported to the Data Protection Commissioner and note their reasons why on the Data Protection Incident Spreadsheet. A completed Notification of Data Breach Form will be saved to the file. See later, 'How to complete the Notification of Data Breach Form'.

Confirmation all incidents reported

Each month the Compliance Officer will contact all staff and ask that they confirm that all Data Protection Incidents, which they are aware of, have been reported. Confirmation of each staff member contacted and each staff member's response, confirming that all incidents have been reported to the Compliance Officer will be recorded and maintained by the Compliance Officer in the appropriate folder.

Analysis

Each month the Compliance Officer will include the following information in the monthly Operations Report for sign-off by the Principal:

- Number of Data Protection Incidents identified
- How many were breaches and how many were non-breaches
- A breakdown of the type of errors made
- What area was responsible for the Data Protection Incident
- How many incidents resulted in a complaint being raised

Recording

All Data Protection incidents will be set up and recorded on the Data Protection Incident Spreadsheet. If a formal complaint has been raised, this should be recorded on the Data Protection Incident Spreadsheet but also logged as a complaint under the customer name and their particular plan number(s). However, if the person who notified us about the incident is not a customer then it should be recorded under the customer name and plan number of the customer whose information was incorrectly disclosed.
The Compliance Officer should set up a complaint file in line with Castle Capital Financial Plannings normal Complaints Processes and Procedures. In this file, copies of all relevant letters, telephones calls, emails and a copy of the Notification of Data Breach Form, should be saved.

Complaint Category and Sub category

All reported Data Protection incidents are reviewed by the Compliance Officer to determine if a customer's data was put risk and if an error occurred. However, while all reported incidents that require action from the Compliance Officer are recorded on the Data Protection Incident and Breaches Grid, not all incidents reported are raised as a complaint.

Therefore, the Compliance Officer has two complaint categories to select from when completing the Data Protection Incident and Breaches Grid:

- Data Protection - Complaint
- Data Protection – No Complaint

Data Protection - Complaint

Use this category only if a Data Protection Incident is reported and a complaint is also being raised, please note upon investigation it is possible that a data protection breach may not have occurred but we should still use this category for reports and trend reviews.

Data Protection – No Complaint

Use this category only if a Data Protection Incident is reported but a complaint has not been raised, please note upon investigation it is possible that a data protection breach may or may not have occurred but we should still use this category for reports and trend reviews.

Example of Data Protection – No Complaint
Person reporting the incident makes us aware that they received post for someone else and just wanted to make us aware of the error. Staff member discovers error that was made and reports incident for investigation.

Within each category the following sub-categories apply

- Error and Breach
- Error but No Breach
- No Error and No Breach

Error and Breach

Use this sub category if we have made a mistake and put a customer's data at risk.

Error but No Breach

Use this sub category if we made a mistake but we did not put a customer's data at risk.

No Error and No Breach

Use this category if we are satisfied having reviewed the incident that no error and no breach occurred.

Data Protection Incidents and Breaches Spreadsheet

The Compliance Officer will maintain a spread sheet called 'Data Protection Incident and Breaches Grid detailing all reported incidents which is saved in the appropriate folder.

This spreadsheet will record all Data Protection Incidents that are reported to the Compliance Officer. The incident should be recorded to the spread sheet immediately and kept up to date as the case progresses.

If *No Breach* has occurred then the Data Protection Incident and Breaches Grid should still be updated to note 'No' Breach has occurred. The notes should be updated to explain why *No Breach* occurred and what action, if any, was taken to correct any errors.

The Data Protection Incident and Breaches Grid is to be used by the Compliance Officer for tracking purposes and must be kept up to date and complete. Each month a check, to identify all incidents that were set up using the complaint category of Data Protection – Complaint, is compared to cases recorded on the Complaint Spreadsheet, to ensure all incidents which were raised as complaints have been correctly recorded. Any Incidents that are recorded on the Data Protection Incident Spreadsheet as a complaint but not recorded on the Complaints Spreadsheet should be reviewed and resolved immediately with follow up corrective actions were appropriate. (Any anomalies should be detailed and recorded as rectified in an appropriate folder)

Handling of Incidents & Breaches

The requirement is to contact all affected parties and bring to their attention what information has been disclosed as soon as possible.

When an incident has been discovered it should be treated with the utmost urgency. All affected parties must be contacted as soon as possible, advised of what happened and what information was disclosed. All efforts should be made to retrieve the data in order to secure the information and reassure the affected parties.

Any system errors must be rectified immediately. If it is not possible to amend these to prevent further possible errors then the Compliance Officer should notify the Principal to determine what temporary measures can be put in place.

A letter should be sent to all affected parties to explain what happened and what steps we have taken to amend this. Where appropriate copies of the information disclosed should be sent to the correct owner, e.g. Copies of letters that were sent or clearly set out details of what information was provided during a telephone conversation.

Ensure when doing this that no details of other customers are disclosed, this may require redacted versions to be provided. Any communications with customers should not refer to regulatory breaches and do not need to note whether or not the incident is being referred to the Data Protection Commissioner.

In offices where there is more than one adviser, give the respective adviser advance notice of what happened and allow them to decide if they should also contact the customer. A copy of the email should be saved to the appropriate folder.

Where a complaint in relation to the data incident has been made, the Consumer Protection Code rules apply and all instances should be handled in accordance with Castle Capital Financial Planning's Complaint Processes and Procedures.

Unless it's clear a complaint was raised, when writing to the person whose information was disclosed they do not need to be advised about the option to refer their case to the Ombudsman as they have not raised a formal complaint and the purpose of this contact is solely to notify them of the error. Should this person reply expressing their dissatisfaction, a, complaint should be set up under their particular plan and handled as per Castle Capital Financial Planning's Complaint Processes and Procedures and it should be noted that the complaint was the result of an error in line with Consumer Protection Code requirements.

Corrective and Preventative Actions

In all cases appropriate corrective action(s) should be identified to address the incident and preventative measures should be taken to ensure no further similar incidents occur. Any errors on systems should be corrected as soon as possible and steps taken to ensure that further data protection breaches do not occur while the incident is being addressed, e.g. incorrect address or wrong customer information must be corrected immediately and / or a system warning note added and / or a total correspondence hold for all affected parties applied.

All Corrective and Preventative Actions identified should be recorded on the Data Protection Incident and Breaches Grid and included on the Notification of Data Breach Form. It is the responsibility of the staff member(s) who receive(s) the Corrective Action to review it and implement suitable measures to ensure further mistakes do not happen. Where Corrective and Preventative Actions have been identified these should be discussed with the relevant staff member(s) and a specific time for resolution / implementation agreed. This date should be noted in the Notification of Data Breach Form and the Compliance Officer will record this in the Data Protection Incident and Breaches Grid. If an issue persists, then the Principal will need to review the situation and take appropriate action in line with Castle Capital Financial Planning's processes and procedures.

Some Examples of Corrective Measures:

- Retrieve and secure disclosed information (if this is not possible should request that recipient confirm they have destroyed the information)
- Inform the affected individual/s (outline what occurred, what was disclosed, apologise)
- Amend or update incorrect records
- Correct system errors
- Highlight issue with individual staff member involved

Some Examples of Preventative Measures:

- Add warning to plan record
- Change or improvement to process or procedures (e.g. introducing spot-check control)
- Additional system controls
- Training

Notification of Data Breach Form

For all breaches, the Notification of Data Breach Form must be completed and saved to the appropriate folder.

If numerous customers had their details disclosed then a separate spread sheet with details of all the affected customers under the same headings in the form should be attached to the Notification of Data Breach Form.

For each reported incident a separate form should be completed.

CASTLE CAPITAL
Financial Planning

Data Retention Procedures

Summary / Purpose	This document sets out the steps regarding the retention and disposal of paper records and electronic documents
Developed By	Castle Capital Ltd & Castle Capital Financial Planning
Target Audience / User	Castle Capital Financial Planning Employees
Date	1st January 2020

Circulation / Sign-Off List	
Document Owner	Castle Capital Ltd & Castle Capital Financial Planning
Distribution List	Castle Capital Financial Planning Employees
Maintenance Cycle	Twelve months The Policy may be reviewed between such intervals in the event of any legislative or other relevant developments.
Document Sign-Off	Castle Capital Ltd
Document Sign-Off Date	1st January 2020
Post Sign-Off Changes to Doc	Jonathan McDonnell 01 January 2020

Document History

Version	Date	Brief description of modification
1.0	1st January 2020	process document

CASTLE CAPITAL
Financial Planning

Table of Contents

CASTLE CAPITAL
Financial Planning

Background

All data created and received in the course of Castle Capital Financial Planning's activities constitute the official records of Castle Capital Financial Planning. The information contained in these records serve as documentary evidence of functions executed and activities performed, and comprises a vital source of knowledge regarding how and why decisions were taken.

The purpose of this Policy is to ensure that necessary records and documents this office are adequately protected and reliably maintained, and to ensure that records that are deemed as no longer needed by Castle Capital Financial Planning are discarded at the proper time and disposed in the appropriate manner. All staff should understand their obligations in retaining paper or electronic documents - including e- mail, Web files, text files, sound and movie files, PDF documents, and any other files.

Applicability

This Policy applies to all physical records and electronic documents, generated in the course of Castle Capital Financial Plannings operations, including both original documents and any reproductions, and defines the retention period of each type of data, according to the rules set in the Data Retention Schedule.

Consideration be given to security, authenticity, accessibility, version control, preservation (e.g. back- up of records) and the disposal of such records.

The objectives of this policy are to:

- support records management within Castle Capital Financial Planning;
- support Castle Capital Financial Planning's administrative and operational requirements, including adherence to Castle Capital Financial Planning's policies and procedures, and compliance with relevant legislation and regulation;
- ensure preservation of records of permanent value and to ensure continued access to appropriate historical / archived records;
- promote day-to-day efficiency and good office management;
- ensure timely destruction of records that no longer need to be retained.

All staff should understand their obligations in retaining paper or electronic documents - including e- mail, Web files, text files, spreadsheets, CCTV, sound and movie files, PDF documents, and any other files and any systems / devices on which such files are held / stored.

Staff must employ the following good housekeeping practices in the management of electronic records;

- sensible and consistent naming of files and folders;
- systematic indexing / classification of records;
- backup of appropriate files on a regular basis;
- delete records regularly (including email records) in accordance with the Data Retention Schedule;
- restricted access to record systems (use of passwords, timed lock out of PCs etc.);
- particularly sensitive records to be emailed to external bodies should be password protected;
- produce paper copies if required to maintain the integrity of manual files, etc;
- In the case of electronic records where the computer equipment is maintained by Castle Capital Financial Planning's IT department or sourced externally through an IT Support Service Company, the office which creates/maintains these records must formally agree a backup and recovery procedure with the Compliance Officer / Principal.

Where electronic records are kept on systems not maintained internally, a formal inventory of such records should be maintained by the Compliance Officer.

Basic Rules

Personal data should never be kept on a "just in case" basis and may only be held for as long as required to meet the legal, administrative, financial and operational requirements of Castle Capital Financial Planning during which time, they should be filed appropriately.

Following a period of time, as set out in the Data Retention Schedule, they are either archived or destroyed; Examples of requirements include but are not limited to;

- legal or regulatory requirements
- legitimate business purposes.
- comply with FSPO requirements on long term investment products or mortgages;
- CBI/CPC requirements on retaining Fact Finds.
- the Data Retention Schedule which sets out the retention periods and their rationale for each category of data.

Administration

The approved maintenance, retention and disposal schedule for physical and electronic records of Castle Capital Financial Planning will be reviewed, administered and implemented to ensure that all staff are compliant with this Policy. Records must be sorted and filed on a basis that ensures efficient retrieval.

- Retention Schedule must be reviewed periodically (best practice is at least annually) to ensure completeness.
- Data must be purged / deleted in line with the Data Retention Schedule and clear responsibility for doing so assigned within Castle Capital Financial Planning.
- Castle Capital Financial Planning must ensure that all paper files, including those kept in archive or off-site storage, are all destroyed securely.

Appendix I: View our Data Retention Schedule

Suspension Events

In the event Castle Capital Financial Planning is served with any complaint, legal notice, request for documents for an investigation or audit, the Compliance Officer / Principal may suspend any further disposal of documents until otherwise determined. Any such suspension will be recorded in the appropriate file with a note to outline Castle Capital Financial Planning's rationale together with a proposed timeframe to recommence the normal retention process.

CASTLE CAPITAL
Financial Planning

Section Topic & Data Type

Examples of section topics might include but is not limited to;

- Accounting and Finance
  - Accounts Payable / Receivable / Budgets / Bank Statements /Payroll / Expenses / Procurement / Fees etc
- Firm Correspondence
  - Routine - notes of appreciation, congratulations, letters of transmittal, and plans for meetings
  - Non-routine - having significant lasting consequences
- Electronic Documents
  - Emails, PDF's, Text files, Web files / cookies
- Customer Data
  - Customer Correspondence / Calls, Financial Reviews, Application Forms, Complaints etc.
- Legal Files and Papers
  - Legal letters, court orders etc.
- Employee Data
  - Employee Personnel Records including attendance records, application forms, job or status change records, performance evaluations, termination letters, rewards, test results, training and qualification records etc.
- Property Records
  - Correspondence, Property Deeds, Assessments, Original Purchase / Sale / Lease Agreement, Property Insurance Policies
- Tax Records
  - Tax bills, Tax returns

Under each of these headings the Compliance Officer / Principal will list out the record types for that category of data and outline a retention period specific to it.

For example

Accounting and Finance

Record Type	Retention Period
Accounts Payable ledgers and schedules	7 years
Accounts Receivable ledgers and schedules	7 years
Annual Audit Reports and Financial Statements	Permanent

CASTLE CAPITAL
Financial Planning

Data Privacy Notice & Procedures

Summary / Purpose	This document sets what we use personal information for and explains a living individual's rights around how we use it.
Developed By	Castle Capital Ltd & Castle Capital Financial Planning
Target Audience / User	Castle Capital Financial Planning Employees
Date	1st January 2020

Circulation / Sign-Off List	
Document Owner	Castle Capital Ltd & Castle Capital Financial Planning
Distribution List	Castle Capital Financial Planning Employees
Security / Confidentiality	Castle Capital Financial Planning Employees
Maintenance Cycle	Twelve months The Policy may be reviewed between such intervals in the event of any legislative or other relevant developments.
Document Sign-Off	Castle Capital Ltd
Document Sign-Off Date	1st January 2020
Post Sign-Off Changes to Doc	Jonathan McDonnell 01 January 2020

Document History

Version	Date	Brief description of modification
1.0	1st January 2020	process document

CASTLE CAPITAL
Financial Planning

Table of Contents

CASTLE CAPITAL
Financial Planning

Background

We know a living individual's personal data is important to them and it is important to us too. Our Privacy Notice tells a living individual what we use their personal data for and explains their rights around how we use it. Please read this Privacy Notice and procedures document to understand how and why we use a living individual's personal data.

We use personal data to provide business services, to meet any legal and regulatory obligations, and for legitimate business reasons; advice, arrange transactions and set up plans, service our customers with advice on claims and encashments.

We pass data to the relevant product producers with whom we hold an agency appointment for the purpose of arranging those transactions and setting up plans.

If we receive personal information about someone else, we must ensure we have their permission and make them aware of our Data Privacy Notice.

CASTLE CAPITAL
Financial Planning

What is Personal Data

Personal Data

Personal data means data relating to a living individual, who is, or can be identified from the data and includes;

- Personal details
- Family and lifestyle details
- Education and training
- Employment details
- Financial details
- Contractual details (for example, goods and services provided to a data subject)
- Online identifiers (IP addresses, cookies)

Sensitive Personal Data

Sensitive personal data is “special categories of personal data” and specifically include medical data. Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing

- Medical details
- political opinions
- religious / philosophical beliefs
- trade union membership
- data concerning health or sex life and sexual orientation
- race / ethnic origin
- genetic data
- biometric data

Automated and Manual Data

Automated Data means information that is being collected or processed by e.g. a computer, operating automatically in response to instructions given for that purpose,
Manual Data means information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system.

Privacy by Design states that any action Castle Capital Financial Planning undertakes that involves processing personal data must be done with data protection and privacy in mind at every step. This includes internal projects, product development, software development, IT systems, and much more. In practice, this means that the IT department, or any department that processes personal data, must ensure that privacy is built in to a system during the whole life cycle of the system or process, rather than tagging security or privacy features on at the end of the process

Privacy by Default means that once a product or service has been released to the public, the strictest privacy settings should apply by default, without any manual input from the end user or data subject. In addition, any personal data provided by the data subject, to enable a product's optimal use should only be kept for the amount of time necessary to provide the product or service. If more information than necessary to provide the service is disclosed, then "Privacy by Default" has been breached.

CASTLE CAPITAL
Financial Planning

Requirements by Law

We must have a lawful basis to collect and use Personal Data

The Data Protection Principles require that we process all personal data lawfully, fairly and in a transparent manner. The individual's right to be informed requires us to provide information about our lawful basis for processing their data and means we need to include these details in our privacy notice.

We must determine the lawful basis before we begin processing

The individual must be informed of the purpose for processing their data before we begin such processing. We must take care to get it right first time. The data processing should be relevant, adequate and limited to what is necessary for its purpose. If we can reasonably achieve the same purpose without the processing, then we don't have a lawful basis.

Request to swap the original purpose

We should not seek to swap to a different lawful basis at a later date without good reason and must always consult the Compliance Officer in any such instance. Should it be deemed necessary for the lawful purpose to change, it may be possible to continue processing under the original lawful basis if the new purpose is compatible with the initial purpose (unless the original lawful basis was *Consent*).

Processing Special Category Data

We need to identify both a lawful basis for general processing and an additional condition for processing this type of data. In order to lawfully process special category data, identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9. NOTE: These do not have to be linked.

The lawful bases for processing include;

- **Consent**: the individual has given clear consent for us to process their personal data for a specific purpose.
- **Contract:** the processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract.
- **Legal Obligation**: the processing is necessary for us to comply with the law Legitimate interests: the processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

The separate conditions for processing include;

- *the data subject has given explicit consent to the processing of those personal data for one or more specified purposes,*
- *processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law*
- *processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;*
- *processing is carried out in the course of its legitimate activities with appropriate safeguards*
- *processing relates to personal data which are manifestly made public by the data subject*
- *processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity*

CASTLE CAPITAL
Financial Planning

Contract

We need to collect and use personal data to provide a plan contract which can include a living individual's:

- name
- date of birth
- contact details
- bank account details
- financial information
- health details
- employment details
- pension and salary information

Personal data needed for plan contracts is held and used to:

- Process an application
- issue a plan
- provide information about the plan
- provide customer care and service
- contact and inform of relevant actions that may need to be taken

Required by Law:

We use personal data to comply with law and regulations;

- reporting to regulators
- maintaining proper records
- Internal reporting, quality checking, compliance controls and audits to help meet our regulatory obligations.
- We must collect certain personal information to comply with Anti-Money Laundering law (Up to date proof of identification and address)
- Customer Due Diligence (Financial Sanctions / Politically Exposed Persons (PEP's) / searches of publicly available information)
- tax residence information and tax identification number for tax reporting
- Personal and financial information in order to complete a financial review and recommend the most suitable financial product for a customer. This involves creating new and assumed personal information, and we will check to see if a customer record already exists.

What is Legitimate Interest

We use a living individual's personal information for our legitimate interests which we believe benefit our customers. We also receive and access information from product producers in order to provide better advice and customer care. We must maintain a record of our assessment so as to demonstrate that we have given proper consideration to the rights and freedoms of individuals involved.

- Employment data processing
- Fraud and financial crime detection and prevention (Anti Money Laundering (AML) requirements)
- processing for the purposes of ensuring network and information security, including preventing unauthorised access to electronic communications networks and stopping damage to computer and electronic communication systems
- Compliance with law enforcement, court and regulatory requirements
- Relations with insurers – information to process insurance claims

- To comply with industry practices (issued by the Financial Action Task Force (FATF), Wolfsburg AML Principles, etc.)
- Modelling – develop or operate financial//conduct and risk models
- Communications & marketing - Direct Marketing OR using summary information to help promote products and services.

Consent

We require consent from a living individual for us to collect and use personal data. We must explain what we need it for and how they can withdraw consent if they change their mind in the future. It must be as easy for them to withdraw their consent as it is to give it.
We must be able to demonstrate that the individual owner of that personal data gave their informed, unambiguous and proactive consent to the processing and we bear the burden of proof that consent was validly obtained. The individual shall also have the right to withdraw their consent at any time, has the right to be forgotten.
The execution of a contract or the provision of a service cannot be conditional on consent to processing or use of data that is not necessary for the execution of the contract or the provision of the service.

Where do we get Personal Data?

Living Individuals provide us with their personal information directly when they contact us, complete our forms, speak with us or visit our website, our social media accounts. For more information on what personal information is collected and used on our website please see our Web Privacy.
We also get personal information from solicitors, employers, and regulators and create new personal information about data subjects based on information they have given us and through their interactions with us.

To Whom do we pass Personal Data

We pass personal information to;

Data processors:

- *Companies that act as service providers under contract with us and only process personal information as instructed by us. All personal information is transferred securely and is not used by other parties for any other reason.*

The categories of services that we use other Data Processors for include;

- *document management, administration, customer services, marketing, Financial Sanctions and PEP checks to comply with Anti-Money Laundering rules and to maintain a list of identified high-risk customers, to comply with legal obligations.*

Product Producers

- *We pass personal information to product producers with whom we hold an agency, in order to arrange transactions agreed with our customers.*

Investment Service Providers;

- *We pass personal information to investment service providers where our customers want to access specialist investment services through their plan e.g. Stockbroker or Online Trading Platform.*

Regulators:

- *We pass personal information to Regulators and the Revenue Commissioners or as needed to comply with regulations and laws.*

Other Companies:

- *We pass personal information to third parties, including other companies with whom we have business arrangements, with the recorded consent of the data subject.*

All personal information is processed and stored within the EU.

How Long do we Keep Personal Data?

We keep and use personal information for as long as a living individual has a relationship with us.

We also hold it after this where we need to for complaints handling, for system back-ups needed for disaster recovery and for as long as we have to under regulations.

We confirm to a living individual how long we will keep personal information for when they avail of a single or specific service such as a quote or call-back on our website.

Living Individual's Rights

Living individuals have a number of rights over their personal information which they can exercise free of charge by contacting us. We will need to verify the identity the data subject in line with our normal DP checks and we will respond within one month in line with the GDPR regulation. Any restrictions to their rights will be explained in our response.

- **Right to Information**
  The information set out in our Privacy Notice. If we update the Privacy Notice, if we change the type of personal information we collect and / or change how we use it, we need to inform the living individual. We have controls in place to protect all personal information and minimize the risk of security breaches. However, should any breaches result in a high risk for the data subject, we will inform them without delay.

- **Right to Restrict or Object**
  Living individuals can restrict or object to any unfair and unlawful collection or use of their personal information. They can object to any automated decision making that has a legal or similar significant impact for them and ask for the decision to be made by a person. They can withdraw consent and object to, for example, *direct marketing*.

- **Right to Correct and Update**
  Living individuals can ask us to correct and update personal information we hold about them. In order to provide them with the best service it is important we have their correct personal information, such as contact details.

- **Right to Delete and Be Forgotten**
  Living individuals can have their personal information deleted if it is incorrect or has been processed unfairly or unlawfully. If they have withdrawn consent they can ask for their personal information to be deleted. We will keep a record of their request so we know why their personal information was deleted. If we have provided a regulated product or service to them, we must keep their personal information for a minimum period by law (e.g. 7 years).

- **Right to Portability**
  Living individuals can ask for a copy of all personal information that they gave us (including through their interactions with us), and which we hold in an automated format. Living individuals can receive this in a machine-readable format that allows them to keep it. They may also request us to send this personal information in a machine-readable format to another company. The format will depend on our ability to provide this in a secure way that protects all the personal information. We will not likely be able to use a copy of any personal information sent to us in this way from another company because we can only collect personal information that we need.

- **Right to Access**
  Living individuals have the right to know what personal information we hold about them and to receive a copy of their personal information.

We must tell them:
— why we hold it;
— to whom we pass it to, including whether we transfer it outside the EU;
— how long we keep it for;
— where we got it from; and

This right does not allow Living individuals to access personal information about anyone else other than themselves.

Please see sections on Data Access Requests and Data Info Enquiry.

CASTLE CAPITAL
Financial Planning

Risk and Control Review / Assessment

Castle Capital Financial Planning will effectively and periodically assess any gaps in our DP Policies; ensuring any and all revisions applicable to GDPR are updated. We will review our firm's framework and best **practices at least annually**, and make any necessary changes and/ or provisions in order to fill any identified gaps.

We will sustain Data management through the monitoring, reviews and communication specific to our firm's data protection framework e.g. recording, monitoring, retention of personal information, monitoring of clear desks, regular data protection training and awareness.

We will align our processes with the Data Protection Principles for any information requests, incident handling and legal compliance e.g. complaints, subject access request, breach reporting processes.

We will routinely review and assess both Internal and external threats to Castle Capital Financial Plannings data security.

One review Maintenance Cycle and Risk Review and assessment will be completed every 12 months.

The timeline for each review cycle should be determined by Castle Capital Financial Planning but should take account of the level of risk associated with each process, ad hoc reviews resulting from a process failure, but also any regulatory or legislative updates as and when they occur. The outcome of the review will be a decision to revise, amend, consider recommendations or reconfirm and approve the existing process document.

Training

There will be Monthly staff meetings held and staff records CPD reviewed on GDPR.

Queries

The Compliance Officer has responsibility for coordination and compliance relating to the administration of all data protection matters, including responding to general queries and requests by Data Subjects relating to personal data as well as requests for assistance from firm employees involved in collecting, storing and processing personal information.

Any queries relating to data protection issues, including requests by individuals for access to and/or correction of any personal data held by Castle Capital Financial Planning and relating to such individuals should be directed to the Compliance Officer Castle Capital Ltd at Castle Capital Financial Planning

CASTLE CAPITAL
Financial Planning

Glossary

In order to comply with regulations and legislation and to give clarity to staff about their role and responsibilities in relation to data protection, Castle Capital Financial Planning recognises the following terms a definition;

- **Data** means information in a form that can be processed. It includes both automated data and manual data.

- **Automated data** means any information on computer, or information recorded with the intention that it be processed by computer rather than by human intervention.

- **Manual data means** information that is recorded as part of a relevant filing system or with the intention that it forms part of a filing system.

- **Relevant filing system** means any set of information that, while not computerised, is structured by reference to individuals, or by reference to criteria relating to individuals, so that specific information relating to a particular individual is readily accessible.

- **Personal data** means data, including sensitive personal data, relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of Castle Capital Financial Planning.

- **Sensitive personal data** relates to specific categories of data, which are defined as data relating to a person's medical health, racial origin; political opinions or religious or philosophical beliefs; physical or mental health; sexual life; criminal convictions or the alleged commission of an offence; trade union membership.

- **Data Controller** processes information about living people. The data controller must be in a position to control the contents and use of a personal data file, i.e. determine the purposes and means of the processing of personal data

- **Data Processor is** a body that processes personal data on behalf of a data controller

- **Data Subject** is an individual who is the subject of personal data (the living individual)

- **Processing** means performing any operation or set of operations on data, comprising;

    - obtaining, assembling, organising and storing data,
    - using, consulting and retrieving data,
    - altering, erasing and destroying data,
    - disclosing data.

While every effort is made to include words / explanations in this glossary that are relevant a contemporary, and consistent with current regulation and legislation, the list is not exhaustive and therefore if any there are any suggestions that any staff member would like added to this glossary, please notify the Compliance Officer. All submissions are greatly appreciated and recorded anonymously.