Lifestyle Financial Planning

Data Protection Policy

Introduction

ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning needs to gather and use certain information about individuals.
These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.
This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards thus complying with the legislation.

Purpose

This data protection policy ensures : ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning

- Comply with Data Protection Legislation and follow Good Practice;
- Protect the Rights of Employees, Customers and Partners;
- Is Transparent in terms of How It Stores and Processes Individuals' Data;
- Protects itself from the Risks associated with a Data Breach.

Background to the General Data Protection Regulation ('GDPR')

The General Data Protection Regulation 2016 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

Policy Statement

The General Data Protection Regulation (GDPR) describes how organisations - including ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning, must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The GDPR Is Underpinned by Six Important Principles Requiring That Personal Data Be:

1. Processed lawfully, fairly and in a transparent manner;
2. Collected for specified, explicit and legitimate purpose;
3. Adequate, relevant and limited to what is necessary;
4. Accurate and where necessary, kept up to date;
5. Retained only for as long as necessary;
6. Processed in an appropriate manner to maintain security.

The Board of Directors of ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning, located at 1 Tintern, Saltmills, New Ross, Co. Wexford, are committed to compliance with all relevant EU and Member State laws in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning collects and processes in accordance with the General Data Protection Regulation (GDPR).

The GDPR and this policy are applicable to all ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning personal data processing functions, including those performed on customers', clients', employees', suppliers' and partners' personal data, and any other personal data the organisation processes from any source.

The GDPR Owner is responsible for reviewing the register of data processing annually, in light of any changes to ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning activities (as determined by changes to the data inventory register and the management review) and to any additional requirements identified by means of data protection impact assessments (DPIA's).

Partners and any third parties working with or for ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning, and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy.

No third party may access personal data held by ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning without having first entered into a data confidentiality agreement, contained in the Data processor checklist which imposes obligations on the third party no less onerous than those to which ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning is committed, and which gives ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning the right to audit compliance with the agreement.

Privacy Policy - Data Protection Principles

1. Be processed lawfully. fairly and in a transparent manner

ES Lifestyle Financial Planning will not process any personal data unless there is a legal basis to do so (under GDPR) such as consent or it is necessary for the performance of a contract[1] . Therefore, processing will be lawful if:

1. The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
2. the data subject has given consent to the processing of his or her personal data for one or more specific purposes (e.g., for marketing purposes).

The GDPR has increased requirements about what information should be available to data subjects, which is covered in the 'Transparency' requirement.

Transparently- the GDPR includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using, clear and plain language.

The specific information that must be provided to the data subject must, as a minimum, include:

- the identity and the contact details of the controller and, if any, of the controller's representative;
- the contact details of the Data Protection Officer;
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- the period for which the personal data will be stored;
- the existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;
- the categories of personal data concerned;
- the recipients or categories of recipients of the personal data, where applicable;
- where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;
- any further information necessary to guarantee fair processing.

2. Personal data can only be collected for specific, explicit and legitimate purposes

- Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the supervisory authority as part of ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning GDPR register of processing.

[1] The other four lawful basis are in short; 1) legitimate interest, 2) it is necessary for compliance with a legal obligation, 3) it is in the public interest and 4) to protect the vital interests of the data subject.

3. ***Personal Data must be adequate, relevant and limited to what is necessary***

- The GDPR Owner is responsible for ensuring that ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning do not collect information that is not strictly necessary for the purpose for which it is obtained.

- All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must include a fair processing statement or link to a privacy statement and be approved by the GDPR Owner.

- The GDPR Owner will ensure that, on an annual basis all data collection methods are reviewed by internal audit to ensure that collected data continues to be adequate, relevant and not excessive.

4. ***Personal data must be accurate and kept up to date with every effort to erase or rectify without delay***

- Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

- The GDPR Owner is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

- It is also the responsibility of the data subject to ensure that data held by ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning is accurate and up to date.

Completion of a registration or application form by a data subject will include a statement that the data contained therein is accurate at the date of submission.

- The GDPR Owner is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date taking into account, the volume of data collected, the speed with which it might change and any other relevant factors.

- On at least an annual basis, the GDPR Owner will review the retention dates of all the personal data processed by, ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning by reference to the data inventory, and will identify any data that is no longer required in the context of the registered purpose.

5. ***Personal data must be kept in a form such that the data subject can only be identified for as long as is necessary for processing.***

- Where personal data is retained beyond the processing date, it will be minimised, encrypted/pseudonymised, in order, to protect the identity of the data subject, in the event of a data breach.

- Personal data will be retained in line with the Retention of Records Procedure and, once its retention date has passed, it must be securely destroyed, as set out in this procedure.

- The GDPR Owner must specifically approve any data retention that exceeds the retention periods defined in the Retention of Records Procedure, and must ensure that the justification is clearly identified, and in line with the requirements of the data protection legislation. This approval must be in written format.

6. **Processed in an appropriate manner to maintain security**
    - In determining appropriateness, the GDPR Owner, should also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or customers) if a security breach occurs, the effect of any security breach on ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning itself, and any likely reputational damage, including the possible loss of customer trust.

When assessing appropriate technical measures, the GDPR Owner will consider the following:

- Password protection;
- Automatic locking of idle terminals;
- Removal of access rights for USB and other memory media;
- Virus checking software and firewalls;

- Role-based access rights including those assigned to temporary staff;
- Encryption of *devices* that *leave* the organisations premises such as laptops;
- Security of local and wide area networks;
- Privacy enhancing technologies such as pseudonymisation and anonymisation;
- Identifying appropriate international security standards relevant to ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning.

When assessing appropriate organisational measures, the GDPR Owner will consider the following:

- The appropriate training levels throughout ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning
- Measures that consider the reliability of employees (such as references etc.);
- The inclusion of data protection in employment contracts;
- Identification of disciplinary action measures for data breaches;
- Monitoring of staff for compliance with relevant security standards;
- Physical access controls to electronic and paper-based records;
- Adoption of a clear desk policy;
- Storing of paper-based data in lockable fire-proof cabinets;
- Restricting the use of portable electronic *devices* outside of the workplace;
- Restricting the use of employees own personal devices being used in the workplace;
- Adopting clear rules about passwords;
- Making regular backups of personal data and storing the media off-site;
- The imposition of contractual obligations on the importing organisations, to take appropriate security measures when transferring data outside the EEA.

- These controls have been selected, based on identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning must demonstrate compliance with the General Data Protection Regulation's other Principles (Accountability)

The GDPR includes provisions that promote accountability and governance. These compliment the GDPR's transparency requirements. The accountability principle in Article 5(2). requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility.

Consent

ES Lifestyle Financial Planning understands ‘consent’ to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject’s wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.

ES Lifestyle Financial Planning also understands ‘consent’ to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the grounds of misleading information will not be a valid basis for processing.

There must be some active communication between the parties to demonstrate “active consent”. Consent cannot be inferred from non-responsive communications. We must be able to demonstrate that consent was obtained for the processing operation.

For sensitive data, explicit consent from data subjects must be obtained unless an alternative legitimate basis for processing exists

Data Subjects' Rights

Data subjects have the following rights regarding data processing, and the data that is recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed;
- To prevent processing likely to cause damage or distress;
- To prevent processing for purposes of direct marketing;
- To be informed about the mechanics of automated decision-making process that will significantly affect them;
- To not have significant decisions, that will affect them, taken solely by automated process;
- To sue for compensation if they suffer damage by any contravention of the GDPR;

- To act to rectify, block, erase, including the right to be forgotten, or destroy inaccurate data;
- To request the Supervisory Authority to assess whether any provision of the **GDPR** has been contravened;
- To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller;
- To object to any automated profiling that is occurring without consent.

Subject Access Requests

All individuals who are the subject of personal data held by ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning are entitled to:

- Ask **what information** the company holds about them and why;
- Ask **how to gain access** to it;
- Be informed about **how to keep it up to date;**
- Be informed about how the company is **meeting its data protection obligations.**

Should an Individual contact the company requesting this information, this is called a Subject Access Request.
Subject Access Requests from individuals should be made by email, addressed to the data controller at elio@eslifestylefinancialplanning.ie. The data controller can supply a standard request form, although individuals do not have to use this.
The data controller will aim to provide the relevant data within **30 days.**
The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Consent

ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning understands 'consent' to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.

ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified
their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the grounds of misleading information will not be a valid basis for processing.

There must be some active communication between the parties to demonstrate "active consent". Consent cannot be inferred from non-responsive communications. The controller must be able to demonstrate that consent was obtained for the processing operation.

For sensitive data, explicit consent from data subjects must be obtained unless an alternative legitimate basis for processing exists.

Security of Data

All Employees/Staff are responsible for ensuring that any personal data that ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning holds and for which they are responsible, is kept securely and is not, under any conditions, disclosed to any third party unless that third party has been specifically authorised by ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning to receive that information and has entered into a confidentiality agreement.

All personal data should be accessible only to those who need to use it, and access may only be granted by the GDPR Owner.

All personal data should be treated with the highest security and must be kept:

- in a lockable room with controlled access; and/or
- in a locked drawer or filing cabinet; and/or
- if computerised, password protected; and/or
- stored on (removable) computer media which are encrypted.

Care must be taken to ensure that PC screens and terminals are not visible except to authorised Employees/Staff of ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning. Screens must lock automatically after a short period of inactivity, and all Employees/Staff must follow the rules in this policy before they are given access to organisational information of any sort.

Manual records may not be left where they can be accessed by unauthorised personnel and may not be *removed* from business premises without explicit *(written)* authorisation. As soon as manual records are no longer required for day-to-day client support, they must be *removed* from secure archiving in line with your policies.

Personal data may only be deleted or disposed of in line with the Retention of Records Procedure.

Records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed, as required before disposal.

Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site.

Disclosure of Data

ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Gardai/Police. All Employees/Staff should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to consider whether disclosure of the information is relevant to, and necessary for, the conduct of ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning business.

All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the GDPR Owner.

ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning Retention and Disposal of Data

shall not keep personal data in a form that permits identification of data subjects for a longer period than is necessary, in relation to the purpose(s) for which the data was originally collected.

ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

The retention period for each category of personal data will be set out in the Retention of Records Procedure, along with the criteria used to determine this period, including any statutory obligations ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning has, to retain the data.

The Retention of Records Procedure will apply in all cases.

Personal data must be disposed of securely, in accordance with the sixth principle of the GDPR. Thus, processed in, an appropriate manner, to maintain security, thereby, protecting the "rights and freedoms" of data subjects. Any disposal of data, will be done in accordance with the Retention of Records Procedure.

Personal Data Breaches

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Examples include an email sent to the wrong person, a lost laptop or phone, or unauthorised access to client files.

Any member of staff who becomes aware of a breach, or a suspected breach, must report it to the GDPR Owner, Elio Lodola, immediately.

The GDPR Owner will act straight away to contain the breach and recover any data where possible, assess the risk to the individuals affected, and record the breach in the firm's breach register, whether or not it needs to be reported.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the GDPR Owner will notify the Data Protection Commission without undue delay and, where feasible, within 72 hours of becoming aware of it.

Where a breach is likely to result in a high risk to individuals, the firm will also inform the individuals affected without undue delay, explaining what happened and what they can do to protect themselves.

After each breach, the GDPR Owner will review what happened and put in place any changes needed to prevent it happening again.

Data Transfers

1. ***Data Transfers between controllers and processors within the EEA***

Where personal data is being processed by a processor on behalf of a controller or is being transferred from the controller to the processor (e.g., to a back-office system provider, data processed via EDI, Insurer, or for Payroll/IT support), you, the broker as data controller, must ensure a 'Standard Contractual Clause' is in place. To be used between the controller and processor in the EEA (not to be used for data transfers to third countries).

These clauses cannot be amended, deleted, or restricted. They can however, be added to, provided that the resulting agreement does not conflict with or contradict the clauses contained within the SCCs.

All exports of data from within the Non-European Economic Area (EEA) countries (referred to in the GDPR as 'third countries') are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects".

The transfer of personal data outside of the EEA is prohibited unless one or more of the following specified safeguards, or exceptions, apply:

An Adequacy Decision

The European Commission can and does assess third countries, a territory and/or specific sectors within third countries to assess whether there is an appropriate level of protection for the rights and freedoms of natural persons. In these instances, no authorisation is required.

Countries that are members of the European Economic Area (EEA) but not of the EU are accepted as having met the conditions for an adequacy decision.

A list of countries that currently satisfy the adequacy requirements of the Commission are published in the *Official Journal of the European Union. (Please see "Related Documentation" section below).*

Assessment of Adequacy by the Data Controller

In assessing adequacy, ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning, as the exporting controller, should consider the following factors:

- the nature of the information being transferred;
- the country or territory of origin, and final destination, of the information;
- how the information will be used and for how long;
- the laws and practices of the country of the transferee, including relevant codes of practice and international obligations.

EU–US Data Privacy Framework

If ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning wishes to transfer personal data from the EU to an organisation in the United States, it should check that the organisation is certified under the EU–US Data Privacy Framework, which the European Commission recognised as providing an adequate level of protection in July 2023. The earlier Privacy Shield framework is no longer valid and must not be relied on. Where the organisation is not certified, another safeguard set out in this section, such as Standard Contractual Clauses, must be in place.

Binding Corporate Rules (BCRs)

ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning may adopt, approved binding corporate rules for the transfer of data outside the EU. This requires submission to the relevant supervisory authority for approval of the rules that ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning is seeking to rely upon.

Standard Contractual Clauses

ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning may use the Standard Contractual Clauses adopted by the European Commission for the transfer of data outside the EEA. Where these clauses are used, the firm will also check that the law of the destination country allows the recipient to comply with them.

Exceptions

In the absence of an Adequacy Decision (including certification under the EU–US Data Privacy Framework), Binding Corporate Rules and/or Standard Contractual Clauses, a transfer of personal data to a third country or international organisation shall only take place on one of the following conditions:

- the data subject has explicitly consented to the proposed transfer, after being informed of the possible risks of such transfers, for the data subject, due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the controller, or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject, between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; and/or
- the transfer is necessary to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

Data flow

ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning has established a data inventory and data flow process as part of its approach to address risks and opportunities throughout its GDPR compliance project namely;

- business processes that use personal data;
- source of personal data;
- volume of data subjects;
- description of each item of personal data;
- processing activity;
- maintains the inventory of data categories of personal data processed;
- documents the purpose(s) for which each category of personal data is used;
- recipients, and potential recipients, of the personal data;
- the role of ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning throughout the data flow;
- key systems and repositories;
- any data transfers;
- all retention and disposal requirements.

ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning is aware of all risks associated with the processing of, specific types of personal data.

ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning assesses the level of risk to individuals associated with the processing of their personal data. Data Protection Impact Assessments (DPIAs) are carried out in relation to the processing of personal data by ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning and in relation to processing undertaken by other organisations on behalf of. ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning

ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning shall manage any risks identified by the risk assessment, to reduce the likelihood of a non-conformance with this policy.

Where a type of processing, particularly using new technologies and considering the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning shall, prior to the processing, carry out a Data Protection Impact Assessment (DPIA) of the impact of the envisaged processing operations on the protection of personal data. A single Data Protection Impact Assessment (DPIA) may address a set of similar processing operations that present similar high risks.

Following the result of a Data Protection Impact Assessment (DPIA), it is clear that ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning is about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as to whether ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning may proceed must be escalated for review to the GDPR Owner.

The GDPR Owner shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the supervisory authority.

Data Protection Risks

This policy helps to protect ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning from potentially, serious data security risks, including:

- **Breaches of confidentiality:** for instance, information processed inappropriately;
- **Reputational damage:** for instance, the Company could suffer material or non-material damage if hackers successfully gained access to sensitive data.

General Staff Guidelines

- The only people able to access data covered by this policy should be those who **need it for their work;**
- Data **should not be shared informally.** When access to confidential information is required, employees can request it from their line managers;
- ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning will provide training to all employees to help them understand their responsibilities when handling data;
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below;
- **Strong passwords are mandatory,** and they should never be shared;
- Personal data **should not be disclosed** to unauthorised people, either within the company or externally.
- Data should be **regularly reviewed and updated.** If it is found to be out of date and/or no longer required, it should be deleted and disposed of appropriately.
- Employees **should request help** from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the GDPR Owner.
When data is **stored in paper format,** it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet;**
- Employees should make sure paper and printouts are **not left where unauthorised people could see them,** like on a printer;
- **Data printouts should be shredded** and disposed of securely when no longer required;
- When data is **stored electronically,** it must be protected from unauthorised access, accidental deletion and malicious hacking attempts;
- Data should be **protected by strong passwords** that are changed regularly and never shared between employees;
- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used;
- Data should only be stored on **designated drives and servers** and should only be uploaded to an **approved cloud computing service.**
- Servers containing personal data should be **sited in a secure location,** away from general office space.

- Data should be **backed-up frequently.** Those back-ups should be tested regularly, in line with the company's standard backup procedures.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by **approved security software and a firewall.**

Data Usage

Personal data is of no value to ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning unless the business can make use of it. However, it is when personal data is accessed and used, that it can be at the greatest risk of loss, corruption or theft. For example:

- When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended.
- Personal data should not be shared informally. It should only be sent by email where the email or attachment is encrypted or password protected, or through a secure portal.
- Data must be encrypted before being transferred electronically. The GDPR Owner can explain how to send data to authorised external contacts.
- Personal data should not be transferred outside the European Economic Area (EEA) unless one of the safeguards set out in the Data Transfers section of this policy is in place.
- Employees **should not save copies of personal data to their own computers.** Always access and update the central copy of any data.

Data Accuracy

The law requires ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning to take reasonable steps to ensure data is kept accurately and up to date.
The higher the importance, that the personal data is accurate, the greater the effort ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning should put into ensuring its accuracy. It is the responsibility of all employees who work with data to take reasonable steps, to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary.** Staff should not create any unnecessary additional data sets;
- Staff should **take every opportunity to ensure data is updated.** For instance, by confirming a customer's details when they call;
- ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning will make it easy for data subjects to update the information ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning holds about them. For instance, via the company website;
- Data should be **updated as inaccuracies are discovered.** For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the GDPR Owner's responsibility to ensure marketing databases are checked against industry suppression files every six months.

Disclosing Data for Other Reasons

In certain circumstances, GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board of directors and from the company's legal advisers, where necessary.

Providing Information

ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How their data is being used;
- How to exercise their rights.

To this end, the company has a Privacy Statement, setting out how data relating to individuals is used by the company.
(This is available upon request. A version of this statement is also available on the Company's website).

Roles and Responsibilities

ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning is a Data Controller under the GDPR.

Top Management and all those in managerial or supervisory roles throughout ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning are responsible for developing and encouraging good information handling practices within ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning; responsibilities are set out in individual job descriptions.

GDPR Owner

The GDPR Owner Elio Lodola have specific responsibilities in respect of procedures such as the Subject Access Request Procedure and are the first point of call for Employees/Staff, seeking clarification on any aspect of data protection compliance.

Compliance with data protection legislation is the responsibility of all Employees/Staff of who process personal data.

The GDPR Owner arranges data protection training and awareness for all Employees/Staff of ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning at least once a year, with additional training for specific roles where needed.

Employees/Staff of ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning are responsible for ensuring that any personal data about them and supplied by them to ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning is accurate and up-to-date.

Everyone who works for or with ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The board of directors is ultimately responsible for ensuring that ES Mortgage and Financial Services Ltd trading as ES Lifestyle Financial Planning meets its legal obligations.
- The GDPR Owner, Elio Lodola, is responsible for:
    - Keeping the board updated about data protection responsibilities, risks and issues;
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule;
    - Arranging data protection training and advice for the people covered by this policy;
    - Handling data protection questions from staff and anyone else covered by this policy;
    - Dealing with requests from individuals to see the data ES Lifestyle Financial Planning holds about them (also called 'Subject Access Requests').
    - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

Definitions

Definitions used by the company drawn from the General Data Protection Regulation (GDPR)

Material scope (Article 2.)

The GDPR applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

Territorial scope (Article 3.)

The GDPR will apply to all controllers that are established in the EU (European Union) who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data in order to offer goods and services, or monitor the behaviour of data subjects who are resident in the EU.

GDPR Article 4. Definitions

Establishment

The main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates to act on behalf of the controller and deal with supervisory authorities.

Personal Data

Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or

more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special Categories of Personal Data

Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data, for the purpose of, uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or

sexual orientation.

Data Controller

The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by European Union or Member State law, the controller or the specific criteria for its nomination may be provided for by European Union or Member State law.

Data Subject

Any living individual who is the subject of personal data held by an organisation.

Processing

Any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means or not, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling

Is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal Data Breach

A breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority where the breach is likely to result in a risk to the rights and freedoms of individuals, and to inform the individuals affected where the risk is likely to be high.

Data Subject Consent

Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

The GDPR and Children

In Ireland, a child is a person under the age of 18, and the digital age of consent is 16 (Data Protection Act 2018). Where an online service is offered directly to a child under 16, processing based on consent is only lawful if consent has been given or authorised by the holder of parental responsibility over the child. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

Third-Party

A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing System

Any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Related Documentation

- ***An Adequacy Decision:*** Please see *The European Commission's adequacy decisions are listed on its website, commission.europa.eu.*
- www.eslifestylefinancialplanning.ie for further information on policies and procedures.

Contacts

Elio Lodola GDPR owner 086 811 4566