Company Policy

General Data Protection Regulation (GDPR)

v18.05
TT & PC

This document outlines the steps taken by Plan Money Ltd to comply with GDPR and details how we deal with any data protection breaches.

Background

All advisers working at Plan Money have processes to follow and policies to uphold as part of the financial planning advice they provide and the transactions they facilitate for clients. This includes obtaining and retaining personal client data which is held in electronic form. Personal data plays a significant role in our financial advice process and is dealt with under the General Data Protection Regulation May 2018, Anti Money Laundering Regulations 2007 and the Serious Crime Act 2015. Prior to holding personal data from our clients and prospective clients, a signed Client Agreement document is obtained, giving permission for us to hold this information for the purpose of financial advice and facilitation to meet our client's expressed financial planning objectives.

The Client Agreement requests client's consent for Plan Money to collect personal data and hold this on our computer database systems. This agreement fully explains why this information is collected and retained. We advise our clients we will be required to renew this information when it becomes out of date or when their financial planning objectives change, leading to the need for further financial advice. We inform our clients that we need to retain this information for a period of time, depending on the regulatory risk factor of the business conducted, in order to satisfy our regulators in the event of the time lapsed if we are asked to deal with a complaint.

Plan Money provides its clients with the freedom to withdraw from this consent where information is not required for a set period of time by us. We understand that by holding personal data we are bound by the new General Data Protection Regulation with regard to informing our clients why we need this information and for how long it is required. We provide the housing of this personal data on our computer server which contains robust anti-virus and back-up measures. We currently use the AVG Antivirus software and a mirror-drive back-up on an on-site Small Business Server.

Our website www.plan-money.co.uk does not currently collect or store client data.
Our emails are hosted by Sys3 Ltd www.sys3.com who have a separate GDPR agreement for the security and confidentiality of our client's personal data held on our server.
Our Client Management system is Intelligent Office provided by Inteliflow. They are an award-winning web-based business management system for financial advisers, keeping all personal data confidential and secure.

Process

Plan Money is a data controller and a data processor in respect of the personal data it receives

Broad outline client personal data is collected at early engagement stage via our All About You document. As more data is collected throughout the investigative stages it is saved in an electronic client file and in a Factfind document.

The identification documentation we collect falls under Money Laundering Regulations and our advisers are required to collect both person/name (picture and signature) identification and address identification under these rules. Our preferred identification choice is usually a copy of passport and a driving licence, but this may also extend to Council Tax bill, bank statement, utility bill, or HMRC documentation. We ensure these documents are in date at the commencement of the client engagement process and when renewing advice or when transacting repeat business. If new copy ID documentation is required, old ID documentation will only be held in an archive folder; a folder which relates to historic advice and/or transactions, or a separate archive ID folder.

Plan Money appreciates that clients may wish to appoint an alternative or complementary Financial Adviser. Upon receipt of such a request, Plan Money will provide their data without undue delay; within a period of one month. This would require formal, quantifiable client permission before doing so. This could be if their Client Agreement with us was terminated by either them or us. We may ask to retain some document to satisfy the regulators request in record keeping in the event of time lapse for future circumstances of an investigation or compliant.

Clients have the option to request that their personal records are deleted from our computer database. For financial advisers where previously advised clients may have recourse on our engagement with them, the request to be wiped from our database can be refused, but only where we will need the data in future circumstances of time lapse.

Potential breach

We have identified circumstances which could be deemed a breach to our GDPR obligations.

- The loss of unencrypted hardware e.g. laptop (containing client data).
- The loss of an unencrypted data storage device e.g. USB stick (containing client data).
- A loss of a mobile device e.g. smart phone (containing client data).
- Where repeat contact is made with a client or potential client where prior consent has not be agreed.
- Cyber attacks, phishing scams, communication hacking.
- Computer virus invasions.
- Any areas where we feel our clients are being placed in a situation where their personal data is not safeguarded.

If Plan Money identifies a breach in our data protection, we will take the following actions:

- We will notify the Information Commissioner's Office (IOC) www.ico.org.uk/Report
- We will make notification within 72 hours of the breach being identified.
- We will notify any clients where the breach has impact on their personal data.
- We will set up an investigation into the breach and keep all records for further inspection.

The inspection into the breach will highlight the cause of the breach and the steps taken to rectify any serious loss of confidentiality/service to our client/s. The Compliance Oversight (Peter Chadborn) will collect relevant information and discuss how to deal with the breach. When we report a breach to the ICO it will therefore include the following details:

- The nature of the breach and details relating to it.
- The client/s whose personal data has been breached and what data this is.
- Confirm we have advised the client/s affected, informing them they may be subject to identity fraud, financial loss, reputational damage or loss of confidentiality.
- Identify the likely consequences of the breach.
- Confirm how we intend to deal with the breach.

Preventative measures

Plan Money Ltd takes all personal data collection and storage very seriously. We aim to retain it only for the purposes of providing accurate and appropriate financial advice and facilitating relevant transactions. Should any member of Plan Money breach the GDPR rules in any way, they must immediately report this to the Compliance Oversight (Peter Chadborn) who will then follow our procedures to collect information and report it accordingly. In his absence they must report to the Compliance and Training Manager (Terri Tilbury) who will then follow our procedures to collect information and report it accordingly.

We have set the following parameters for all members of Plan Money to reduce the likelihood of a GDPR breach.

Circumstance / Issue	Advisers	Non-Advisers
Collecting copies of client ID	May capture on smart phones. Must be emailed and stored on PM server within 48 hours and then all records must be deleted from smart phone. May capture via email or post.	 May capture via email or post only.
Client contact details (telephone, address, email).	May be held on smart phone but limited to essential contact information. May not be held on laptop or data storage device. It is Adviser's responsibility to ensure smart phone is secured with password (or similar security) and that device requires password if idle for period of time. Also that device contains anti-virus software.	May not be held on smart phone, laptop or data storage device.
Client files (paper)	Must be stored securely when not in use. If taken away from office (client meetings or home-working) must be transported securely and stored securely and only kept away from office for time that is reasonable to fulfil the remote working requirement. Must not be stored in vehicle.	Must be stored securely when not in use.
Client files (electronic)	Must not be copied onto any device.	Must only be accessed in the office during course of work and working hours.
Hardware	Laptops, home computers or mobile devices used to access client data while working remote, must be secured with password (or similar security) and device must require password if idle for period of time. Device must also contain anti-virus software.	Must only be accessed via PM work station, in the office, during course of work and working hours.
Remote access	Only pre-approved methods of accessing client data must be used. E.g. secure VPN, smart phone.	