Money Advice Data Handling Policy

Version 1.0.3

Version **1.0.4**

Change History

VERSION NUMBER	AUTHOR	DATE	REASON FOR ISSUE	CHANGES
1.0	Diarmuid O'Connor	9/6/2011	1st Draft	
1.0.1	Satheesh Vattem	1/12/2011		Updated Money Advice address
1.0.2	Satheesh Vattem	2/3/2013		Updated Opsource new details
1.0.3	Satheesh Vattem	1/1/2015		Updated reference to Caledonian to Royal London
1.04	Satheesh Vattem	1/09/2017		Updated Money Advice address

Table of Contents

1. Introduction

The purpose of this document is to outline the process involved in Money Advice providing up to date client policy data from insurance companies to brokers, and the policies related to this data

We will identify the various data transfer methods involved, and specify how this data will then be processed, stored and ultimately made available to the brokers using Money Advice software applications.

1.1 Scope

This policy applies to all Money Advice employees who access, process, or store client policy data.

2. Background

The Money Advice offices are based at Staion Road, Ennis, Co. Clare.

The Money Advice+CRM application and database are hosted on servers in a data centre operated by Dimension Data (previously known as Opsource (www.dimensiondata.com) in the UK. Dimension Data are a SAS 70 certified company.
Money Advice's contract with Dimension Data is for a "managed hosting" service – this means that Dimension Data have full responsibility for security and maintenance of the hardware.

The insurance companies participating in this process are as follows:
Aviva
Friends First
Irish Life
New Ireland
Standard Life
Zurich Life
Royal London

3. Broker Authorisation

In order to receive their client policy data in The Money Advice+CRM application, brokers will have to complete an authorisation form. On this authorisation form they will specify the insurance companies that they deal with and the agency codes that they hold with these insurers

Money Advice will then provide these authorisation forms to the insurance companies. When the companies receive a new form detailing the agency codes, they will update their own internal processes so that the client policy data associated with the matching agency code appears in the bulk data file that they provide to Money Advice.

As a result, the data files that Money Advice will receive will be bulk files containing client policy data belonging to a number of brokers. Money Advice will develop extract processes and scripts to then extract this data into their own databases based on the agency codes provided. The processes and scripts used in this process will contain validation checks to ensure the integrity of the data being processed

The insurance companies will carry out validation on any agency codes provided to them by Money Advice. This will prevent the scenario of a broker being provided with incorrect data.

4. Outline of the Download Process

The process of making the data available to the brokers involves 3 steps

1. Download the data from the insurers directly to the Money Advice hosted servers
2. Process the data files using the extract routines
3. Transfer the data to the SQL Server database tables

Money Advice will have 2 dedicated managers with responsibility for processing this

data. The data will be received from the insurance companies in a variety of manners:

Format	Description	Automatic process
VPN	Bulk data files will be downloaded from provider server after connecting using VPN client software with secure logon	No
Secure FTP	Money Advice will automatically download the data file using Secure FTP software	Yes
Website (HTTPS)	Money Advice will log on to the provider website and download the bulk data file	No
Secure email	Data files will be sent using a secure encrypted email. The password for the email will be sent to Money Advice via SMS	No

Once the data files have been processed, and the data is residing in the SQL Server database they will then be deleted

5. Policy in relation to Data Storage, Access and Confidentiality

In respect of the client policy data received from insurance companies, Money Advice shall undertake to:

- Treat data received from providers as confidential and will not use it for any purpose other than to make it available to brokers via our software applications
- Allow brokers access only to the data which is associated with their supplied and agreed Agency Codes
- Deny brokers access to data which is not associated with their supplied and agreed Agency Codes

To achieve these undertakings, Money Advice have implemented a specific policy in relation to data security. The goal of the data security policy is to protect the confidentiality, integrity and availability of the client policy data. The creation of this policy reflects the level of impact to Money Advice Limited if confidentiality, integrity or availability of the data is compromised.

	Potential Impact		
Security Objective	Low	Medium	High
Confidentiality- Preserving authorized restrictions on information access and disclosure.	The unauthorized disclosure of information could be expected to have a limited adverse effect on Money Advice operations.	The unauthorized disclosure of information could be expected to have a limited adverse effect on Money Advice operations.	The unauthorized disclosure of information could be expected to have a limited adverse effect on Money Advice operations.
Integrity- Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on Money Advice operations.	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on Money Advice operations.	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on Money Advice operations.
Availability- Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on Money Advice operations.	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on Money Advice operations.	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on Money Advice operations.

The following are the guidelines which we Money Advice have applied in relation to the client policy data.

Security Category	Specific Guidelines
Access Controls	Viewing and modification restricted to authorised individuals as needed for business-related roles Project Manager grants permission for access Authentication and authorisation required for access Confidentiality agreement signed by all employees
Copying/Printing (applies to both paper and electronic forms)	Data should only be printed when there is a legitimate need Copies must be limited to individuals authorised to access the data and have signed a confidentiality agreement Data should not be left unattended on a printer/fax
Network Security	Protection with a network firewall required IDS/IPS protection required Servers hosting the data cannot be visible to the entire Internet Must have a firewall ruleset dedicated to the system The firewall ruleset should be reviewed periodically
System Security	Must follow OS-specific best practices for system management and security

	Host-based software firewall required Host-based software IDS/IPS recommended
Virtual Environments	May be hosted in a virtual server environment All other security controls apply to both the host and the guest virtual machines Cannot share the same virtual host environment with guest virtual servers of other security classifications
Physical Security	Hosted in a Secure Data Centre required Physical access must be monitored, logged, and limited to authorized individuals 24x7
Remote Access to systems hosting the data	Restricted to local network or secure VPN group Unsupervised remote access by third party for technical support not allowed Two-factor authentication recommended
Data Storage	Storage on a secure server required Storage in Secure Data Centre required Should not store on an individual workstation or mobile device (e.g., a laptop computer) Encryption on backup media required Paper/hard copy: do not leave unattended where others may see it; store in a secure location
Transmission	Encryption required (for example, via SSL or secure file transfer protocols) Cannot transmit via e-mail unless encrypted and secured with a digital signature
Training	General security awareness training required for all employees
Mobile Devices	It is not permitted to store any client policy data on mobile devices