Minerva Personal Data Retention Policy & Cleansing

Introduction

There are 6 main areas covered by this document:

1. How long do we keep data for?
2. How do we handle cases that did not proceed (declined quotes)?
3. How do we correctly implement the 'right to be forgotten' requirement under data protection legislation?
4. How do we store data that is live in the system?
5. How do we handle and store backups?
6. Data stored by sub processors

When we talk about Minerva, we are covering 2 main applications known as:

1. The Minerva Quote Portal (Legacy LFS (Law Firm Services))
2. The Minerva Client Portal

Main policy (Live Cases) How long do we keep data for?

Within the legal process, cases can have differing data retention rules depending on the type of case. However, the data retention provided by Law Firm Services Limited is only in relation to how long the data is stored on our servers given that the "Minerva data" will have been transferred or downloaded (either as data or PDF) to the law firms main data centre which will typically be their own case management system. Minerva therefore does not have a different policy per case type.

When we refer to data retention, we are referring to cases that have proceeded through the system (i.e. a won quote and/or a portal account has been created and/or tasks have been performed).

The section below covers data retention where a case/quote was declined or lost by the law firm.

Data will be retained for a period of 7 years taking into account our data protection obligations, including to keep data for no longer than is necessary for the purposes for which it is processed, balanced against our business requirements to retain the data and the technical and organisational measures involved in deletion. On a monthly basis any data which is over 7 years old will be removed from both the Quote Portal and the Client Portal. This data removal includes the case records and any corresponding documents related to that case.

To implement a consistent policy, we use the 'Creation Date' of the record as the filter. 7 years or more from Creation Date all data will be fully removed.

Within the Client Portal we will purge the case data and documents although we will not remove the login account from the portal only any case data over 7 years old. This enables the same portal account to be used in the future if required.

A Minerva customer may, on request, wish to shorten the data retention timeframe. This would be at an additional cost to them as bespoke routines would need to be created to support this.

Cases that do not proceed

There are multiple reasons why a case may not proceed including the following:

- Client declines the quote
- Law firm Loses the quote via the Quote Portal

There are 2 stages to the data retention for cases that fall into this 'lost' category. The first stage will anonymise the data by using an obfuscation procedure and this will be done after a period of 12 months. The second stage is the same as the Live Cases policy above whereby after 7 years the data and documents are fully deleted.

For cases that are lost the data is anonymised to allow for historic reporting on quotes sent vs won and various other reports. The data obfuscation will obfuscate any client details such as names, address, email address etc including any quote documents. For cases that do not proceed there will be no way to identify who the client was after 12 months.

A Minerva customer may, on request, wish to shorten the data retention timeframe for lost quotes. This would be at an additional cost to them as bespoke routines would need to be created to support this.

Right to be forgotten

If a client of a law firm submits a request to have their data removed via data protection legislation the law firm can submit a request to Law Firm Services Limited that this data is removed. Within the Client Portal the data will be completely removed including their account details. Data in the Quote Portal will be anonymised so that the law firm's existing reports will not be affected.

To initiate a 'right to be forgotten' request it will be necessary to contact the Data Protection Officer 'dpo@lawfirmservices.co.uk'. Law Firm Services Limited will then manage the routine.

In addition we will also need to do a search across all emails for the client in the current system so they can be removed too if it falls within the data retention period of the email system. The current email system has a retention policy of 30 days and we currently do not archive emails.

Data Backups

Backups are handled automatically within the Azure cloud platform. We currently retain backups for a period of 12 months. The right to be forgotten does not extend to our backups currently but in the event of a disaster recovery any previous right to be forgotten requests would be replayed on any restored backups.

Live Data Storage

Data is stored within Microsoft Azure SQL Server databases. All data is encrypted at rest and access to the data is restricted via secure accounts and IP address restrictions.

Documents are stored within Microsoft Azure Storage Accounts. Data is encrypted at rest and only accessible via the security controls provided by the Azure Platform.

Emails are processed through the SMTP2Go system and secured via their platform and accessed via a provided API.

Sub Processors

Minerva uses the following sub processors, and their policies are outlined below:

Credas for ID checks

Hold data for a period of 5 years.

SMTP2Go for email

Hold copies of all emails sent for a period of 30 days. We currently do not use their archiving facility.

Armalytix – for source of funds checks

Banking details are not retained, the summary reports are held for a period of 6 years while the clients own details are held for 3 years.

Yoti for electronic signatures

Controlled via their API so we will manage this in line with our own policies.

FormEvo for Land Registry forms

Currently 7 years which is in line with the HMRC.