Fluent Mortgages Horwich Limited

Data protection audit report

November 2023

Information Commissioner's Office

Executive Summary

Background

The Information Commissioner is responsible for enforcing and promoting compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA18), the Privacy and Electronic Communications Regulations (PECR) and other data protection legislation. Section 146 of the DPA18 provides the Information Commissioner's Office (ICO) with the power to conduct compulsory audits through the issue of assessment notices. Section 129 of the DPA18 allows the ICO to carry out consensual audits. The ICO sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach. High standards of personal data protection compliance help organisations innovate and deliver great services by building trust with the public. The ICO's expertise and consistent approach to regulation provides certainty enabling organisations to feel confident to use personal data responsibly, innovate and support economic growth.

The ICO received two complaints from members of the public, in January and April 2023, relating to disclosures of personal data to third parties. The disclosures had the potential to result in significant harm to individuals. A third complaint was received which related to the withholding of call recordings following a subject access request (SAR) received by Fluent Mortgages Horwich Ltd (FMHL) from a customer.

The ICO were keen to ensure appropriate measures were in place to mitigate the risk of a similar occurrences in future. This assurance was not fully obtained through the ICO's complaint handling process as responses from FMHL demonstrated misconceptions existed in their interpretation of data protection legislation. FMHL were invited to participate in a consensual audit of their processes and procedures.

The ICO's assurance team contacted FMHL in July 2023 and FMHL accepted the invitation to participate in an audit. FMHL cooperated fully with auditors and engaged well with the ICO throughout the audit process. The audit took place at FMHL's headquarters on 13 September.

The purpose of the audit was to provide the Information Commissioner with an assurance of the extent to which FMHL, within the scope of the audit, is complying with data protection legislation and assist FMHL in

identifying and mitigating compliance risks in their current procedures. Following the complaints FMHL have developed an Enhanced Transparency Model (ETM) to improve the provision of information relating to the processing they carry out to their customers. The ETM has not been fully implemented yet as FMHL presented their proposal to the ICO during the audit and will incorporate feedback and audit findings prior to embedding it into their systems. The audit considered what was 'in place' at the time it took place.

Scope

The scope of the audit covered the following key control areas:

a. Governance

The extent to which information governance accountability, policies and procedures, training, risk management, performance measurement controls and reporting mechanisms to monitor data protection compliance to both the UK GDPR and national data protection legislation are in place and in operation throughout the organisation.

b. Lawful basis for processing

The organisation has identified and documented appropriate lawful bases for the processing activities undertaken.

c. Transparency

The provision of clear and concise privacy information to individuals which ensures that the organisation is transparent about their processing of personal data.

d. Data supply and sharing

The design and operation of controls to ensure the receipt and sharing of personal data with processors or other data controllers complies with the principles of all data protection legislation.

e. Data Breach Management

The extent to which effective processes and procedures exist to ensure data breaches are identified, managed and reported in

compliance to both the UK GDPR and national data protection legislation.

f. Information rights requests

The extent to which the organisation is able to provide responses to individuals who exercise their information rights within the requirements of data protection legislation.

The purpose of the audit is to provide the Information Commissioner with an assurance of the extent to which the FMHL, within the scope of this audit, is complying with data protection legislation. This audit report documents our findings within the scope areas covered at the time of the audit.

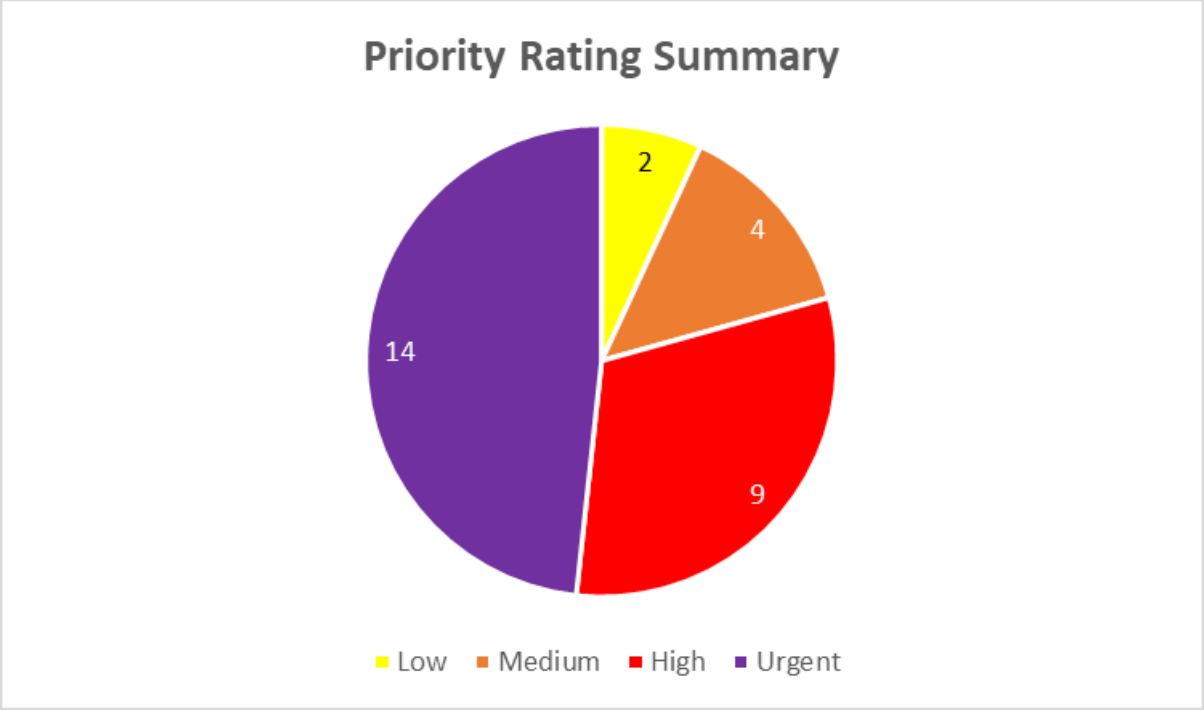
The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures and interviews with selected staff.

Priority of recommendations summary

Where opportunities for improvement were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist FMHL in implementing the recommendations, each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. FMHL's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

Urgent priority recommendations are intended to address risks which represent clear and immediate risks to FMHL's ability to comply with the requirements of data protection legislation.

A summary of the ratings assigned within this report is shown below.



The pie chart above shows a breakdown of the priorities assigned to the recommendations made. There are 14 urgent, 9 high, four medium and two low priority recommendations.

Urgent Priority Recommendations - These recommendations are intended to address risks which represent clear
High Priority Recommendations - These recommendations address risks which should be tackled at the earliest
Medium Priority Recommendations - These recommendations address medium level risks which can be tackled over
Low Priority Recommendations – These recommendations represent enhancements to existing controls to

Areas of good practice

During the audit, ICO auditors were impressed with some of the measures adopted by FMHL to achieve compliance with data protection legislation. These include:

- FMHL have a proactive approach to data protection and have developed a robust organisational structure which ensures data protection matters are discussed at all levels and oversight of performance is achieved at the highest level.
- Compliance with internal policy and legislative requirements are regularly tested and reported on by a dedicated compliance team.
- FMHL maintain various quality certifications to enhance and assure the approach to managing information. These include ISO9001, ISO23001 and ISO27001.
- Data protection is discussed at the beginning of any new project or processing initiative.
- General data protection training is mandatory and completion statistics are monitored closely and non-completion followed up swiftly.

Areas for improvement

The ICO are encouraged by the willingness of FMHL to engage with the audit process and the positive approach they have adopted to improving data protection practices. However, the audit identified some areas where further improvements are required to achieve compliance with data protection legislation.

- Whilst the approach to training is good, the content may not be sufficient to provide staff with a knowledge of data protection that is aligned to the processing carried out by FMHL. Particularly staff who may have more specialist roles such has handling SARs or carrying out DPIAs. More detailed or sector specific training content will help prevent misconceptions about data protection legislation develop within FMHL.

- FMHL have not clearly documented all of their processing activities in a Record of Processing Activities (RoPA) as they are required to do so in Article 30 of the UK GDPR. This means that processing activities and purposes may not all be correctly identified. As a result, they may not have identified a lawful basis for all of their processing or be able to ensure that all requirements of data protection legislation have been applied across all of their processing activities.

- FMHL's fair processing notices FPNs do not contain all the requirements of Article 13 of the UK GDPR. Additionally, the manner in which they are presented means that the information within them may not be immediately understood or transparent to readers.

- Data protection impact assessment methodology is not always granular or objective enough to ensure an effective assessment of risk is caried out.

The matters arising in this report are only those that came to our attention during the course of the audit and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place rest with the management of Fluent Mortgages Horwich Ltd.

We take all reasonable care to ensure that our audit report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report