

Equifax Limited

Data protection audit report Executive Summary

Onsite audit: August 2018

Published: October 2020

1. Background

- 1.1 The Information Commissioner is responsible for enforcing and promoting compliance with the General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA18) 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.
- 1.2 Equifax obtains, processes and shares personal data in service of its three main lines of business; as a credit reference agency (CRA), as a fraud prevention agency, and for marketing services.
- 1.3 As a result of data protection concerns raised in other data broker investigations, the Information Commissioner issued an assessment notice to Equifax in July 2018 concerning the processing of data for the following purposes:
 - direct marketing,
 - lead generation,
 - data broking,
 - personal data pooling, enhancing, enriching, matching, appending, profiling, screening, licensing or selling for any of the above purposes
- 1.4 In November 2018, Privacy International issued a complaint to the Information Commissioner concerning the processing of personal data by Equifax for marketing purposes. The complaint was wide-ranging, covering alleged failures to comply with the data protection principles and individual rights contained in the GDPR. Although our audit work predated this complaint, there is significant overlap between the complaint and our existing work, so for the avoidance of doubt this report also comprises our response to the Privacy International complaint.
- 1.5 The audit field work was undertaken at the Equifax office at 6 Wellington Place, Leeds, LS1 4AP between 28 and 31 August 2018.

2. Scope of the audit

2.1 As per the assessment notice, this audit focuses on Equifax's marketing services and addressed the following data protection risk areas:

- Fairness and transparency
- Lawful basis for processing
- Data protection by design and default
- Creation, maintenance and accuracy of records
- Managing data supply, data enrichment and licensing
- Data subject rights (not including subject access requests)
- Compliance and assurance

2.2 The services in the scope of this audit are characterised as data broking for direct marketing purposes. The ICO has adopted the following definition of data broking:

“data broking” refers to the practice of obtaining information about individuals and trading, including by licensing, this information or information derived from it as products or services to other organisations or individuals. Information about individuals is often aggregated from multiple sources, or otherwise enhanced, to build individual profiles.’

2.3 Equifax collected personal data from third party suppliers, the open electoral register and publicly available data. Equifax used the data to build datasets that they licensed to a number of clients and a small number of resellers (primarily for the open electoral register), who themselves further licensed the data. The datasets enabled organisations to identify new prospective customers and added more detail to clients' existing customer or potential customer lists. Data was licensed for postal marketing only.

Credit reference data was used for limited purposes to confirm and trace postal addresses for marketing and to screen out individuals from clients' postal marketing campaigns based on elements of their credit reference files which might indicate affordability concerns.

Equifax also used personal data to create aggregated and anonymous profiling models which could be applied at postcode level, which it licensed to assist clients with their postal marketing.

3. Audit Approach

- 3.1 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, on-site visits including interviews with selected staff, and an inspection of selected records.
- 3.2 The purpose of the audit was to provide the Information Commissioner with an assurance of the extent to which Equifax, within the scope of this audit, is complying with the GDPR and the DPA18.
- 3.3 The ICO's intention, at the start of the audit process, was to follow our established procedure of making recommendations to address identified weakness and seek a management response.
- 3.4 However, as we compiled the report and considered the evidence supplied concerning Equifax's marketing activities, we were concerned about significant failures to comply with key aspects of the data protection legislation, such that it would not be appropriate to merely issue recommendations that Equifax adjusts its processing.
- 3.5 Accordingly, a Preliminary Enforcement Notice was issued to Equifax in April 2019. A preliminary enforcement notice outlines to an controller that the Commissioner is minded to issue an enforcement notice in respect of her concerns, and sets out the action she intends to require of them. The controller is invited to make representations to the Commissioner on the contents of the notice and proposed remedial actions before a final decision is made on serving the notice. On the basis of Equifax's representations, Equifax's actions to resolve identified issues and subsequent substantial discussions, a revised Draft Enforcement Notice was issued to Equifax in April 2020.
- 3.6 Following the service of the Preliminary and Draft Enforcement Notices, Equifax resolved all of the Commissioner's concerns, in part by terminating much of their data broking for marketing purposes. Although Equifax has changed the nature of their processing, their position is and always has been that they do not accept that they were in breach of data protection legislation.
- 3.7 The summary of key areas for improvement and of good practice given below are those areas that we identified **at the time of the audit** in 2018. In each case, those concerns have been resolved since 2018.

4. Summary of audit findings

Areas for improvement

The Commissioner did not consider that individuals would expect their personal data to have been used for some of Equifax's marketing services. Equifax failed to provide sufficient transparency information to a large number of data subjects whose data was gathered into their marketing services. The existing mechanisms for providing this information were insufficient to meet Equifax's obligations under the transparency, fairness and lawfulness principle or Article 14.

[The Commissioner is satisfied that this has now been rectified, by the termination of all processing that would require notification]

Equifax used credit bureau-derived personal data for limited direct marketing purposes. Credit data was not sold in bulk for these purposes, but was used to verify that address details were correct, to screen individuals out of marketing if their data suggested they might struggle to afford the product or service, and to build anonymised geodemographic models. This was against the reasonable expectations of individuals and in breach of the transparency, fairness and lawfulness principle.

[The Commissioner is satisfied that this has now been rectified, by the termination of the processing in question]

Equifax failed to provide convincing evidence that it had a lawful basis for processing personal data for its marketing purposes. Auditors found the application of the GDPR consent requirements problematic, and the use of the legitimate interest lawful basis was not underpinned by legitimate interest assessments (LIAs).

[The Commissioner is satisfied that this has now been rectified, in part by the termination of the processing in question and by the implementation of valid LIAs]

The systems for recording and applying requests by data subjects to exercise their rights, particularly the right to object to direct marketing, were improperly implemented.

[The Commissioner is satisfied that this has now been rectified]

Areas of good practice

Equifax evidenced a GDPR-readiness programme that, whilst failing to address the matters noted above, did improve the previous processing operations, including requiring more of data suppliers and terminating contracts with organisations not willing to comply.

Auditors were impressed with Equifax's information asset register, the data inventory, which recorded in great detail the information held by Equifax and the interconnections between assets and products, and delivered clear benefits in the management and governance of that data.