Information Commissioner's Office

Investigation into data protection compliance in the direct marketing data broking sector

October 2020

ico.
Information Commissioner's Office

Foreword

Transparency is a central tenet of data protection law: people have a right to expect organisations to be clear, open, and honest with them about how their personal data is being used.

This is important, even where people do not have a direct relationship with the organisation processing their data.

The ICO is committed to intervening where the public do not have access to clear information about how their data is being used. Without transparency, people cannot assert their rights. Our investigation into data analytics for political campaigns is an example of where invisible processing and profiling prevented people from exercising their data protection rights. At that time, we announced that we had served assessment notices to Experian, Equifax and TransUnion (formerly Callcredit) in order to investigate our concerns about the trade in personal data. This report, alongside the enforcement notice and audit executive summaries reveal our findings.

The data broking sector provides a valuable service to support organisations across the UK. Products designed for marketing purposes can have a utility beyond merely sending people promotional material, and are sometimes used to help organisations including charities, health bodies and police forces to target resource to a particular area. But the sector does this by processing large amounts of people's data, often to profile them, and with typically no direct relationship with those people whose information it relies on.

Mass processing of personal data for these purposes, without adequate transparency, is out of line with the reasonable expectations of the public. For some people, this is likely to cause distress.

Our initial investigatory work revealed concerns around how data brokers were obtaining and using people's data, as well as lawfulness, fairness and transparency.

After serving the assessment notices, we conducted audits of the direct marketing data broking business of the three largest credit reference agencies (CRAs) in the UK: Experian, Equifax, and TransUnion.

Although the CRAs varied widely in size and practice, we found significant data protection failures at each company.

Between the CRAs, the data of almost every adult in the UK was, in some way, screened, traded, profiled, enriched, or enhanced to provide direct marketing services. We found that data provided to each CRA in order for them to provide their statutory credit referencing function was being used in limited ways for marketing purposes. The data is used by commercial organisations, political parties for political campaigning, or charities for their fundraising campaigns. But few people are aware that this processing is taking place because they haven't been informed.

Some of the CRAs were also using profiling to generate new or previously unknown information about people, which is often privacy invasive. We have taken action to require change within these companies.

Through our audit and engagement work, many of these concerns have been resolved. Equifax and TransUnion ceased the supply of non-compliant products and services and I am encouraged to see the two organisations committed to complying voluntarily, without the need for enforcement action.

Whilst Experian has made progress in improving its compliance with data protection law, their processing of personal data in the context of their marketing services remains non-compliant with the data protection law. As such, I have issued Experian with an enforcement notice. I believe this is the most effective and proportionate way to achieve compliance in this case, whilst still having a dissuasive and informative impact.

Our action represents a key milestone in driving proportionate and effective change in the direct marketing data broking sector on behalf of consumers. What the CRAs were doing was unlawful; but their trade in personal data with other organisations has implications beyond the industry. Disrupting the flow of non-compliant personal data will have significant impact not just across the sector but will drive benefits for individuals and organisations wherever this data is used.

We remain committed to securing compliance across the data broking sector through further investigative, engagement and educational work. We will publish further audit findings when they are concluded.

Elizabeth Denham CBE
Information Commissioner

Contents

Executive summary

The Information Commissioner has conducted an investigation into data protection compliance in the data broking sector, specifically the provision of offline marketing services by key data brokers.

Data broking involves collecting data about individuals from a variety of sources, then combining it and selling or licensing it to other organisations. 'Offline' marketing services, as referred to in this report, focus on providing marketing to individuals through methods other than the internet.

In the UK there is a large, well-established trade in personal data by data brokers both between themselves and other organisations. It is a complex ecosystem of companies who offer data broking services, ranging from very large multi-national companies to small UK firms.

The scale and the scope of the processing is significant, involving the personal data of millions of individuals – almost every adult in the UK. However this ecosystem, and an individual's place in it, is largely unknown to the general public.

Whilst there are numerous companies acting as data brokers, our investigation initially focused on some of the key players, and this report covers our findings. Specifically, we have investigated the offline direct marketing services of the three largest credit reference agencies (CRAs) in the UK; Experian Limited, Equifax Limited, and the relevant entities within the TransUnion group of companies (TransUnion International UK Limited and Callcredit Marketing Limited).

We have also investigated the direct marketing services of three other data brokers who do not operate as CRAs. We will publish the audit summaries for these three data brokers and communicate any further findings, once we have completed this work.

The ICO recognises that data broking can be positive, for businesses and individuals, however, data brokers must comply with data protection law.

We conducted audits of the direct marketing services of the CRAs. Although there were a wide variety of differing practices across the CRAs,

our investigation revealed systemic compliance failings at each company. Our key concerns were about:

- transparency of the processing;
- Article 14 of the GDPR and invisible processing;
- using credit reference data for limited direct marketing purposes; and
- appropriate lawful bases for processing.

Some of these concerns have been proactively resolved by the CRAs after we informed them that these were serious enough to warrant enforcement action.

Although we have made recommendations to the entire credit reference industry, it is clear that there was a wide variety of differing practices within these businesses, and not all CRAs operated practices which were equally concerning.

Key findings

Key finding 1: The privacy information of the CRAs (in the context of their marketing services) did not clearly explain the processing. CRAs have to revise and improve their privacy information. Those engaging in data broking activities must ensure that their privacy information is compliant with the GDPR.

Key finding 2: In the context of their marketing services, the CRAs were incorrectly relying on an exception from the requirement to directly provide privacy information to individuals (excluding where the data processed has come solely from the open electoral register).To comply with the GDPR, CRAs have to ensure that they provide appropriate privacy information directly to all the individuals for whom they hold personal data in their capacity as data brokers for direct marketing purposes. Those engaging in such data broking activities must ensure individuals have the information required by Article 14.

Key finding 3: The CRAs were using personal data collected for credit referencing purposes for limited direct marketing purposes. The CRAs must not use this data for direct marketing purposes unless this has been transparently explained to individuals and they have consented to this

use. Where the CRAs are currently using personal data obtained for credit referencing purposes for direct marketing, they must stop using it.

Key finding 4: None of the consents reviewed by auditors and relied on by Equifax were valid under the GDPR. To comply with the GDPR, CRAs must ensure that the consent is valid, if they intend to rely on consent obtained by a third party. Those engaging in data broking activities must ensure that any consents they use meet the standard of the GDPR.

Key finding 5: With respect to their direct marketing services, Legitimate interest assessments (LIAs) conducted by the CRAs were not properly weighted. The CRAs must revise their LIAs to reconsider the balance of their own interests against the rights and freedoms of individuals. Where an objective LIA does not favour the interests of the organisation, the processing of that data must stop until that processing can be made lawful. Those engaging in data broking activities must ensure that LIAs are conducted objectively, taking into account all factors.

Key finding 6: In some cases Experian was obtaining data on the basis of consent and then processing it on the basis of legitimate interests. Switching from consent to legitimate interests in this situation is not appropriate. Where personal data is collected by a third party and shared for direct marketing purposes on the basis of consent, then the appropriate lawful basis for subsequent processing for these purposes will also be consent. Experian must therefore delete any data supplied to it on the basis of consent that it is processing on the basis of legitimate interests.

Action taken by the Commissioner

The Commissioner issued preliminary enforcement notices to the three CRAs outlining the steps we intended to require of them and inviting representations.

All three made improvements to their marketing services business on the basis of our findings. In the cases of TransUnion and Equifax, they made improvements alongside withdrawing certain products and services, which together brought them into compliance with the law. It was therefore not necessary for us to issue enforcement notices to TransUnion or Equifax.

Although Experian made progress in improving its compliance, we continue to have a number of fundamental concerns with its processing of personal data. In order to secure compliance, we have issued an enforcement notice to Experian.

Conclusions

We recognise the value of data broking, but in order for it to have a positive impact, the activity must be carried out in compliance with the law.

Our investigation found widespread and systemic data protection failings across the sector. This is particularly concerning in an industry that is entirely dependent on personal data.

We are committed to driving proportionate and effective change across the sector to protect information rights for the millions of data subjects affected. Although our investigation into the data broking activities of the CRAs has concluded, our work in this area continues. We will continue to educate and enforce, where necessary, in order to ensure that data brokers and those who use their services comply with data protection law.

1. Introduction

1.1 About this report

This report focuses on the Commissioner's investigation into the offline marketing services of the data broking industry and, in particular, the activities of the UK's three largest credit reference agencies (CRAs) within this industry; Experian Limited, Equifax Limited, and the relevant entities within the TransUnion group of companies (TransUnion International UK Limited and Callcredit Marketing Limited).

It is important to note that this investigation has focused on the CRAs' data broking for direct marketing activities, and not their core credit referencing function.

'Offline' marketing services, as referred to in this report, focus on providing marketing to individuals through methods other than the internet. This can include postal, telephone and SMS marketing. It also means that the focus of the profiling activities we investigated and address in this report does not include data collected about an individual's online behaviours. We are investigating participants in the online advertising industry separately.

This report provides background information on the law and our investigation, discusses the key findings, outlines the action we have taken, provides conclusions, and outlines next steps.

As well as this report we have also published the executive summaries of the audits undertaken and the enforcement notice issued by the Commissioner. This report is concerned with the thematic issues; the audit executive summaries provide information about the specific processing of each CRA.

1.2 What is data broking for direct marketing purposes?

The ICO has adopted the following definition of data broking for direct marketing purposes, based on our knowledge of the industry:

> '"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.'

Data broking for direct marketing purposes involves collecting data about individuals from a variety of sources, then combining it and selling or licensing it to other organisations. The data broking industry can provide a variety of different services such as:

- selling lists of contact details;
- selling copies of the open electoral register;
- profiling and data enrichment (eg adding data to the profile you already hold on people);
- data matching (eg providing phone numbers for people who you only hold address details for);
- data cleansing and tracing (eg removing deceased records from your database and tracking down new contact details for people);
- screening and suppression services (eg checking the telephone numbers you hold against those registered with the Telephone Preference Service); and
- audience segmenting or other profiling (eg identifying or targeting sub-groups within an audience for tailored messaging).

Some data brokers, such as those we have investigated here, operate 'offline' data broking services, as defined in section 1.1 of this report. Others operate 'online' services, incorporating data about an individual's online behaviours.

In general, data brokers do not engage in marketing in their own name, but rather they provide data analytics to further the direct marketing activities of third parties. For example, these services are used by commercial organisations, political parties for political campaigning, or charities for their fundraising campaigns. However, this data analytics processing by the data broker is still for direct marketing purposes.

In many instances data brokers do not have a direct relationship with individuals and do not collect data directly from them, but instead rely on data collected from other sources, such as:

- publicly available personal data;
- the Open Electoral Register (which can be sold to any organisation for a wide range of purposes);
- third party organisations (eg competition or lifestyle survey companies); and
- personal data supplied by other data brokers.

The activities covered by data broking can vary significantly. Some brokers conduct straightforward activity, such as collating lists of individuals' names and contact details which they sell to organisations. The organisation then uses these details to contact individuals to market their products. These lists are sometimes screened by the broker against databases such as the Telephone Preference Service (TPS) or Mail Preference Service (MPS) to ensure that they exclude individuals who have opted out of unsolicited marketing.

Some data brokers combine multiple sources of data to build detailed profiles of an individual. This can include basics such as names and addresses, combined with further information such as whether they have children, whether they own a car, their perceived likes and dislikes or shopping habits. This more detailed information can be more valuable, as organisations can then target their marketing campaigns more accurately.

In some cases, data brokers use personal data to create geo-demographic models. For example, data is modelled at a postcode level rather than attributed to a specific individual. They sell these products to organisations who, in some cases, attach the modelled attributes to individuals and use the resulting profiles to target those individuals.

1.3 Scale of data broking in the UK

In the UK there is a large, well-established trade in personal data by data brokers, both between themselves and other organisations. It is a complex ecosystem of companies who offer data broking services, ranging from very large multi-national companies to small UK firms.

The three large CRAs in the UK – Experian, Equifax and TransUnion – also operate as data brokers. Other companies solely operate as data brokers, while others offer additional data services as well, such as ID verification and anti-money laundering products. Still more organisations participate in data broking alongside offering more traditional goods or services.

The scale and the scope of the processing is significant, involving the personal data of millions of individuals – almost every adult in the UK.

Many different types of organisation seek to use their services for different purposes, including for direct marketing. For example, our previous investigation into the use of data analytics in political campaigns saw how some political parties purchased data sets from data brokers for election and campaign purposes.

1.4 Action we've previously taken

The ICO has previously issued monetary penalty notices against four UK data brokers, resulting in £640,000 in fines.

- The Data Supply Company (£20,000) in February 2017
- Verso Group (UK) Limited (£80,000) in October 2017
- Lifecycle Marketing (Mother and Baby) Ltd (trading as Emma's Diary) (£140,000) in August 2018
- Bounty (UK) Ltd (£400,000) in April 2019

We issued these fines under the Data Protection Act 1998, which has since been replaced by the GDPR and DPA 2018.

We have served one further data broker based in Canada, AggregateIQ Data Services Ltd, with an enforcement notice under the GDPR. We issued this as part of our investigation into the use of data analytics for political purposes.

There is more information on action we've taken on our website.

2. Legislative framework

2.1 Data protection legislation

The Information Commissioner is the UK regulator of the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA 2018). The ICO also regulates e-Privacy law, which in the UK is the Privacy and Electronic Communications Regulations 2003 (PECR).

Article 5 of the GDPR sets out seven key principles which lie at the heart of the general data protection regime:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

Lawfulness, fairness and transparency are a key part of data protection law. The three elements of lawfulness, fairness and transparency overlap, but all three must be satisfied. It's not enough for an organisation to show processing is lawful if it is fundamentally unfair to, or hidden from, the individuals concerned. These provisions are also a key part of the findings of this investigation.

Failure to comply with the GDPR and DPA 2018 can lead to enforcement action from the Commissioner.

2.2 Lawfulness

For processing to be lawful, organisations need to identify specific grounds for the processing. These are in Article 6 of the GDPR and are known as 'lawful bases'. There are six lawful bases for processing and the most appropriate will depend on the organisation's purpose and relationship with the individual.
If an organisation does not have a valid lawful basis then that particular processing of personal data will be unlawful.

In the data broking context, the lawful bases that are generally referred to are consent (Article 6(1)(a)) and legitimate interests (Article 6(1)(f)).

Consent means offering individuals real choice and control. The GDPR sets a high standard for consent and it must be freely given, specific, informed and unambiguous. It must be a positive opt-in and also be easy to withdraw consent.

Legitimate interests is likely to be appropriate when organisations are using personal data in ways that individuals would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing. There are three elements to legitimate interests. Organisations need to:

- identify a legitimate interest;
- show that the processing is necessary to achieve it; and
- balance it against the individual's rights and freedoms.

Lawfulness also means organisations not doing anything with the personal data that would breach other laws.

2.3 Fairness

Organisations need to demonstrate that they are using personal data fairly. This means that they must be open and honest and not process data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned.

Assessing whether personal data is being processed fairly depends partly on how the organisation has obtained it. Fairness is fundamentally linked to transparency.

2.4 Transparency

Transparency is a key element of the GDPR. As part of this, the GDPR gives individuals the right to be informed about the collection and use of their personal data. It applies both to personal data collected directly from the individual (Article 13) and when it is collected from another source (Article 14).

Achieving transparency also forms part of our strategic goals as a regulator; to increase the public's trust and confidence in how data is used and made available. Without transparency, trust and confidence can be severely impacted. There is more information on the importance of transparency as part of the ICO's regulatory strategy in our Information Rights Strategic Plan 2017-2021.

Organisations must provide individuals with certain information about what they intend to do with their data including the purposes for processing, retention periods and who they will be share it with. This is known as 'privacy information'. Organisations must be clear, open and honest about how they will use personal data. They should draw attention to any processing that is unlikely to be expected by individuals or will have an impact on them.

Transparency is always important, but is particularly important in situations where there is no direct relationship between the organisation and the individual. In these cases, the organisation will have obtained the personal data from another source and the individuals may have no idea that the organisation has collected it and is using it, unless the organisation tells them. If an organisation fails to tell people that they are processing their personal data, this is sometimes known as 'invisible processing'.

Invisible processing results in a risk to the individual's interests as they cannot exercise any control over the organisation's use of their data. In particular, individuals are unable to use their data protection rights if they are unaware of the processing. For example, individuals cannot object to processing if they do not know that it is happening. This also highlights the importance of action from the regulator.

Where individuals are not informed about who is processing their data, what they are doing with it and why, it is hard to argue that the processing is fair and within the reasonable expectations of the individual.

There are exceptions to the requirement for an organisation to provide privacy information if the data is collected from another source. These include where:

- the individual already had the information (Article 14(5)(a)); or

- providing the information to the individual would involve disproportionate effort (Article 14(5)(b)).

For Article 14(5)(a) to apply, the organisation must be able to demonstrate and verify what information the individual already has about the processing and ensure that they have already been given all the information that is listed in Article 14.

For Article 14(5)(b) to apply, the organisation must assess whether there is a proportionate balance between the effort involved to give privacy information and the effect of the processing on the individual.

2.5 Profiling

Profiling is defined in Article 4(4) of the GDPR as:

> "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."

Profiling is where the behavioural characteristics of individuals are analysed, for example to:

- find out about their preferences;
- predict their behaviour;
- make decisions about them; or
- classify them into different groups or sectors.

Profiling for direct marketing purposes often involves predictions, inferences or assumptions about individuals.

Profiling can be beneficial to both the organisation and the individual. However, where profiling takes place without the individual's knowledge or outside of their reasonable expectations, this can result in harm.

A key information rights risk presented by profiling is its intrusiveness. As profiling can generate new or previously unknown information, it can often be highly privacy-invasive. This risk is amplified if profiling takes place without the knowledge of the individual. This removes assurances that can be provided through adequate transparency and creates harm through individuals' loss of control of their personal data.

Profiling often uses inferred, derived or predicted data. It can sometimes be possible to infer special category data, such as information about a person's health, sexuality or political views. Special category data is subject to additional safeguards under the GDPR. It is therefore crucial that individuals understand how and when an organisation can obtain or deduce this data and what purposes they could use it for.

2.6 Individual rights

The GDPR provides individuals with rights in regard to their personal data, including:

- Article 13 – the right to be informed about the collection and use of their personal data where the data is collected directly from the individual;
- Article 14 – the right to be informed about the collection and use of their personal data where the data is collected via another source;
- Article 15 – the right of access to their personal data;
- Article 21(2) – the right to object to the processing of their personal data for direct marketing purposes; and
- Article 17 – the right to have their personal data erased.

2.7 Assessment notices

Section 146 of the DPA contains a provision for the Commissioner to issue an assessment notice. This is, essentially, a notice which we issue to a controller or processor to allow us to assess whether they are compliant with data protection legislation. The notice may, for example, require the controller or processor to give us access to premises and specified documentation and equipment, and make relevant staff available to us for interview.

We may serve an assessment notice at our discretion during any investigation into compliance with data protection law. We will have regard to what action is appropriate and proportionate, including (but not limited to) circumstances where:

- we have intelligence that a controller or processor is not processing personal data in compliance with the law;
- It is necessary to verify compliance with an enforcement notice; or
- the controller or processor has failed to respond to an information notice within an appropriate time.

The notice specifies the times or a time period within which a controller or processor must comply with the requirements we set out.

Failure to comply with an assessment notice can bring about further action, including a monetary penalty. Organisations may appeal assessment notices to the First-Tier Tribunal (Information Rights).

There is more detailed information about assessment notices in our Regulatory Action Policy.

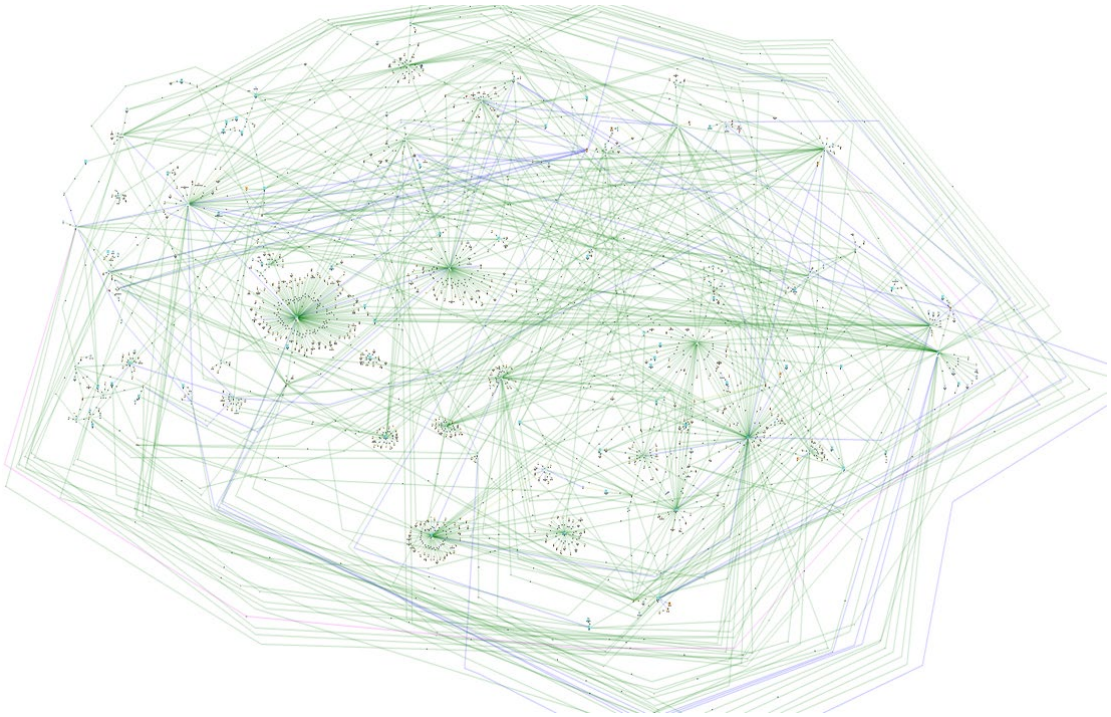
3. Intelligence gathering

3.1 Initial concerns

The ICO has been concerned about the trade in personal data for some time. Our proactive investigative work seeding personal data online revealed concerns with how it is obtained and used, as well as with transparency. Intelligence from this investigative work combined with what we gleaned through investigating concerns from members of the public about unsolicited marketing communications, led the Commissioner to subsequently open an investigation into data broking for direct marketing purposes.

3.2 Call for evidence

In 2015, the ICO began gathering intelligence about the way personal data is traded in the UK. We requested information on a voluntary basis from 1,182 organisations who had registered with us advising that they traded in personal data. We used the information to create a 'map' of the industry and to risk assess individual organisations. This was complex process which significantly improved our understanding of the sector.



Mapped interactions between organisations trading and sharing in personal data (snapshot from 2015)

This map highlighted the circular nature of the trade in personal data, and also the significance of a number of 'hubs' within the sector. These hubs' appeared to have large volumes of data flowing in and out of them, making it clear that they played an important part in the ecosystem. We noted that three of the hubs were the three CRAs – Experian, Equifax and TransUnion (formerly Callcredit). We therefore requested more detailed information from the key players we identified during the mapping exercise.

Given the significance of the three CRAs within the data broking ecosystem, we contacted them again in 2017 to ask further detailed questions about sources of personal data, the products they offered and how they ensured compliance with data protection legislation.

We analysed their responses, and identified areas of significant concern requiring further investigation.

We were also aware that as the GDPR would be coming into force within the next six months, there would be greater value in investigating the practices which would continue after this time, rather than looking into procedures for compliance which were likely to change soon.

3.3 Data analytics for political purposes

Some of the concerns we identified with particular organisations were relevant to our investigation into data analytics for political purposes, and we were therefore able to pursue lines of enquiry as part of that investigation. We used this intelligence to inform our review of data broking and target particular areas of concern.

4. ICO investigation

4.1 Scope of the investigation

Our investigation looked at the provision of offline marketing services by key data brokers. It focused on processing of personal data in the UK about individuals in the UK.

The scope of the investigation did not cover online data broking. It also did not extend beyond looking at the provision of marketing services by the data brokers. In the context of the CRAs, this means that the investigation did not look at their credit referencing functions. The findings set out below therefore do not relate to the credit referencing functions of the CRAs.

4.2 Decision to audit

In summer 2018 after a review of the intelligence we then held, the Commissioner exercised her power to undertake compulsory audits and issue assessment notices to the three CRAs. This allowed us to collect accurate, detailed and up-to-date information about their processing activities.

The Commissioner also decided to investigate practices at three of the non-CRA hubs of data broking we had previously identified, in order to provide contrast to the CRAs' compliance and an overview of data protection compliance more widely across the sector. After reviewing current intelligence, we issued assessment notices to three data brokers of concern.

We announced our decision to conduct compulsory audits of the three CRAs in our 2018 report 'Investigation into the use of data analytics in political campaigns', as we investigated some of the organisations as part of our work on the use of personal data for political purposes.

4.3 The audits

4.3.1 Equifax

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.

4.3.2 Experian

Experian collected personal data from third party suppliers, the open electoral register and publicly available data. Experian used the data to build datasets that they licensed to a comparatively large number of clients and resellers, who themselves further licensed the data. The datasets enabled organisations to find new prospective customers and/or to enrich existing or potential customer data with socio-demographic attributes. Experian also operated data pools with partner organisations.

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

Experian 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 marketing.

4.3.3 TransUnion

TransUnion collected personal data from the open register and publicly available data. TransUnion used the data to build datasets added more detail to a small number of clients' existing customer or potential customer lists, but did not provide individuals' information for prospecting (save for the provision of the Open Register). Data was licensed for postal marketing only.

Credit reference data was used for limited purposes for a handful of clients in order to remove previous addresses from marketing lists and to screen out individuals from clients' marketing campaigns based on elements of their credit reference files which might indicate affordability concerns.

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

4.4 Public awareness

It is likely that the vast majority of UK adults currently appear, or have previously appeared, within the databases of at least one data broker. However, this ecosystem and an individual's place in it are largely unknown to the general public. Because of this lack of visibility and knowledge, the ICO is less able to rely on our usual indicators of the public's opinion, such as complaints made to us. Similarly, as many individuals are unaware that their data is being bought and sold in this way, it is very difficult for individuals to understand who has possession of their personal data in order for them to exercise their information rights.

The ICO commissioned Harris Interactive to undertake a survey in early 2019 to help us understand public awareness and perceptions of data broking. This, in turn, helped to inform our decision-making at that time.

The key findings were that many people were unclear about what exactly happens to their personal data once they have shared it with organisations and generally do not consider that the balance of providing this information is solely in their favour. The majority of respondents considered that any organisation they do not have a direct relationship with should tell them that it has collected and is processing their data.

The results of the research commissioned by the ICO are on our website.

In addition to this subject-specific research, we have gained more insight into the public's view on data broking through intelligence we gathered from the ICO's Annual Track survey. This is a survey we commission each year to help us understand the public's views on information rights issues. In 2020, our findings revealed that only 20% of people surveyed agreed that they would be fine with being contacted by an organisation they had not dealt with before who had bought their details from a partner organisation.

Similarly, only 24% of individuals surveyed agreed that they were fine with being contacted by an organisation they had not dealt with before who had obtained their information from a publicly available source.

There is more about our 2020 Annual Track survey on our website

4.5 Decision to enforce

Our investigation revealed systemic compliance failings within each of the CRAs data broking businesses, particularly for the lawfulness, fairness and transparency principle of the GDPR. Our findings are discussed in detail in section 5 of this report.

These key concerns were deeply embedded in each business. Comprehensive change was required in order to achieve compliance. Given the severity of our findings, in April 2019 we provided each of the three CRAs with a preliminary enforcement notice which set out our concerns, the steps we required them to take, and a clear timescale for compliance, alongside our detailed audit report.

5. Key findings

5.1 Findings of non-compliance

Our investigation revealed systemic compliance failings at each of the CRAs. Our key thematic concerns were consistent across all three, although there were material differences at each organisation.

Many of these concerns have been proactively resolved by the CRAs after we informed them that these were serious enough to warrant enforcement action. In some cases, one or more of the CRAs chose to cease the relevant processing entirely.

5.2 Transparent processing

Transparency is a key requirement of the GDPR. As part of this, individuals have the right to be informed about the collection and use of their personal data. This applies regardless of whether the personal data is obtained directly from the individual or from other sources.

Organisations must be as transparent as possible about the personal data they are using, where they have obtained it from and the ways they will use it. They must be clear and upfront, explaining what they are doing in a way that individuals can readily understand.

Our investigation found that the CRAs did provide some privacy information on their websites about their data broking activities, and links to this information were given by the organisations that supplied data to them. However, this information was not clear because it was not sufficiently prominent, it did not sufficiently explain how the data was collected, what sources were used, how it was processed, or how it was sold.

Key finding 1
The privacy information of the CRAs did not clearly explain their processing with respect to their marketing services.

CRAs have to revise and improve their privacy information.

Those engaging in data broking activities must ensure that their privacy information is compliant with the GDPR.

In response to our findings the CRAs have undertaken extensive work to improve the privacy information available on their websites. We have not needed to enforce our requirements on the CRAs where they have resolved the problematic processing (because they made significant changes, or else they terminated the products in scope).

5.3 Article 14 and invisible processing

The GDPR requires that where organisations obtain personal data from sources other than the individual, they must provide privacy information to individuals within a reasonable period, and at the latest within a month of obtaining their data (Article 14).

If privacy information is not actively provided then this can cause 'invisible' processing – it is 'invisible' because the individual is not aware that the organisation is collecting and using their personal data.

Individuals do not always have a direct relationship with the CRAs in their capacity as data brokers. The personal data they collect is obtained from other sources rather than directly from individuals.

The CRAs did not proactively provide privacy information to individuals when they collected their data from other sources to use for direct marketing purposes.

In some instances they claimed that it was not necessary to provide the information. They felt that the exception at Article 14(5)(a) applied because the individual would already have the information set out in Article 14. The CRAs were therefore relying on the privacy policies of the third parties who were supplying the data to them.

However the privacy policies of third parties did not clearly draw attention to the processing by the CRAs for these purposes. Individuals would only discover it was happening if they reviewed the third party's policies and followed links within those policies.

Individuals are likely to expect that the CRAs process their personal data for credit referencing purposes. However, they are unlikely to expect that the CRAs are processing their data for direct marketing purposes in their capacity as data brokers and building up extensive profiles on them.

The CRAs also claimed that directly telling individuals would involve 'disproportionate effort' (Article 14(5)(b)) due to the large volume of people whose data they hold, the costs associated with making each person aware of the processing and the value that individuals would derive from being told about the processing.

Individuals can exert little or no control over their personal data when they have not been told that their data is being processed and lack understanding of how it will be used or shared. They are also unable to exercise their data protection rights, such as the right to object.

Very large numbers of individuals cannot be the deciding factor against it being proportional to notify people about the processing in these circumstances. Otherwise this would give controllers a perverse incentive to gather as much data as possible in order to reduce the burden on them to notify people.

The nature of the processing that is being undertaken for data broking purposes means that it is likely that the CRAs will have relevant contact details for the individuals affected.

Taking all this into account, it would not be 'disproportionate' for the CRAs to comply with Article 14 and proactively tell people that they are processing their personal data.

Key finding 2

In the circumstances we assessed the CRAs were incorrectly relying on an exception from the requirement to directly provide privacy information to individuals (excluding where the data processed has come solely from the open electoral register or would be in conflict with the purpose of processing – such as suppression lists like the TPS).

To comply with the GDPR, CRAs have to ensure that they provide

appropriate privacy information directly to all the individuals for whom they hold personal data in their capacity as data brokers for direct marketing purposes.

Those engaging in data broking activities must ensure individuals have the information required by Article 14.

In some cases, CRAs made changes in response to our findings on this point. We have not needed to enforce this requirement where they have resolved the non-compliant processing (because they made significant changes, or else terminated the products in scope).

5.4 Using credit reference data for limited direct marketing purposes

The CRAs have a somewhat unique position of holding financial records on the majority of the adults in the UK in their credit referencing capacity, as well as operating data broking businesses alongside this.

Credit referencing helps lenders to ensure that they provide credit responsibly. Individuals benefit from the ease with which their creditworthiness can be evidenced and assessed through this system, but have no choice about whether their data is shared with CRAs for credit referencing purposes if they want to access credit from lenders. The CRAs' pivotal role in the financial sector puts them in a position of trust and this brings responsibilities.

It is therefore crucial that the CRAs are held to high standards of accountability, transparency and fairness. This maintains public trust and confidence both in the important credit referencing service they provide and their data broking activity.

Our investigation found that there data was shared between these two sides of their businesses and personal data held for credit reference services was also being used for some limited direct marketing purposes.

For example, they used personal data from credit referencing to screen individuals out of receiving direct marketing, on the basis of their financial standing. Providing data to help make decisions about who should not

receive direct marketing is a form of selection and is processing for direct marketing purposes.

There were a relatively small number of direct marketing uses made of credit reference data (credit data was not sold in bulk for direct marketing purposes, for example). However, the CRAs did not make clear to individuals that they would use the credit data for direct marketing purposes as part of their data broking business and they did not ask individuals to agree to this use of that data.

Individuals would not expect that their data, which they are required to provide to the CRAs as part of the credit process, to be used for marketing purposes. It is not fair to use their credit data for such a purpose. It is therefore not appropriate for credit reference data to be used by CRAs for marketing purposes unless the individuals have consented to this use.

Key finding 3
The CRAs were using personal data collected for credit referencing purposes for direct marketing purposes.

The CRAs must not use this data for direct marketing purposes unless this has been transparently explained to individuals and they have consented to this use.

Where the CRAs are currently using personal data obtained for credit referencing purposes for direct marketing, they must stop using it.

In some cases, CRAs made changes in response to our findings on this point. We have not needed to enforce this requirement where they have resolved the non-compliant processing (because they made significant changes, or else they terminated the products in scope).

5.5 Lawful basis for processing

The Commissioner's investigation found that the CRAs did not properly assess their lawful basis when processing for direct marketing purposes.

The CRAs did not use the same lawful basis in the same way. We saw three key compliance issues that are outlined below.

Consent

Equifax claimed that personal data was supplied to it by third party data brokers on the basis of consent and it subsequently relied on this consent to process for data broking purposes.

However our investigation found that none of the consents reviewed by auditors met the standard required by the GDPR. For example, the consents were not informed or specific.

This meant that it was processing the personal data without a valid lawful basis.

Key finding 4
The consents relied on by Equifax were not valid under the GDPR.

To comply with the GDPR, CRAs must ensure that the consent is valid, if they intend to rely on consent obtained by a third party.

Those engaging in data broking activities must ensure that any consents they use meet the standard of the GDPR.

We have not needed to enforce this requirement as Equifax has resolved the non-compliant processing.

Legitimate interests

In some instances, CRAs were processing the personal data they held for direct marketing purposes on the basis of their legitimate interests.

The CRAs assessed whether legitimate interests applied to their processing by conducting legitimate interest assessments (LIAs). However, they gave little weight to the fact that they were processing a large amount of personal data in highly targeted ways, profiling individuals, along with significant issues of non-transparency.

Key finding 5
Legitimate interest assessments (LIAs) conducted by the CRAs in respect of their marketing services were not properly weighted.

The CRAs must revise their LIAs to reconsider the balance of their own interests against the rights and freedoms of individuals in the context of their marketing services. Where an objective LIA does not favour the interests of the organisation, the processing of that data must stop until that processing can be made lawful.

Those engaging in data broking activities must ensure that LIAs are conducted objectively taking into account all factors.

In some cases, CRAs made changes in response to our findings on this point. We have not needed to enforce this requirement where they have resolved the non-compliant processing (because they made significant changes, or else they terminated the products in scope).

Using consent then legitimate interests

Our investigation found that in some instances personal data was shared with Experian by third parties on the basis of the individual's consent. But once Experian had obtained this data, it relied on legitimate interests for its own processing activities.

Where data is collected or shared for the purposes of direct marketing on the basis of consent, then the appropriate lawful basis for the subsequent processing for direct marketing purposes will also be consent. Switching from consent to legitimate interests meant that the original consent was no longer specific or informed, the degree of control and the nature of the relationship with the individual was misrepresented, and the right to withdraw consent was also undermined.

This misrepresentation and the impact on the effectiveness of consent withdrawal mechanisms causes a problem with the LIA balancing test. This means that it would inevitably cause the balance to be against the CRA.

In addition, the consents that the third parties were relying on when they supplied the personal data did not constitute valid consent under the GDPR.

Key finding 6
In some cases Experian was obtaining data on the basis of consent and then processing it on the basis of legitimate interests. Switching from consent to legitimate interests in this situation is not appropriate.

Where personal data is collected by a third party and shared for direct marketing purposes on the basis of consent, then the appropriate lawful basis for subsequent processing for these purposes will also be consent.

Experian must therefore delete any data supplied to it on the basis of consent that it is processing on the basis of legitimate interests.

6. Action we've taken

6.1 Powers of the Commissioner

The GDPR and DPA 2018 grant a range of regulatory powers to the Commissioner including assessment notices, enforcement notices and monetary penalties.

The Commissioner's primary aim is to secure compliance with the laws she oversees. This means that we will select the most appropriate regulatory tool for achieving this aim. There is more information about the Commissioner's powers and how she uses them in our Regulatory Action Policy.

As a result of the findings from the audits of the CRAs in their capacity of data brokers, we determined that the infringements warranted further action from the Commissioner.

When deciding which regulatory tool was appropriate in order to secure compliance, we considered a monetary penalty. However, the Commissioner decided that on this occasion an enforcement notice would be the most effective and proportionate way to achieve compliance, whilst still having a dissuasive and informative impact.

An enforcement notice requires an organisation to take specific steps within a certain period of time. As such, they can be a powerful tool to drive change within an organisation. If an organisation fails to comply with an enforcement notice, the ICO is able to issue a fine of up to 10 million Euros, or 4% of the organisation's total annual worldwide turnover, whichever is the greater.

We were conscious that the CRAs have profited from the non-compliant processing identified. However, we have balanced this against the possible cost to them of complying with the requirements we have set out, which is likely to be significant.

6.2 Voluntary compliance

We notified all three CRAs of our intention to take enforcement action on the basis of our audit findings in April 2019. We issued preliminary enforcement notices to Equifax, Experian and the relevant entities within the TransUnion group of companies (TransUnion International UK Ltd and CallCredit Marketing Limited), alongside our audit reports, outlining the steps we intended to require of them and inviting representations.

After a lengthy period of engagement on our findings and intention to enforce, all three CRAs made improvements to their marketing services business. In the case of TransUnion and Equifax, they made improvements alongside the withdrawal of non-compliant products and services, which together brought both into compliance with the law. It has therefore not been necessary to issue enforcement notices to either TransUnion or Equifax in order to achieve compliance.

Although Equifax and TransUnion have 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.

Whilst Experian has made progress in improving its compliance with data protection law, we continue to have a number of fundamental concerns with its processing of personal data which means we have had to take further action in order to secure compliance. It has therefore been necessary for us to issue Experian with an enforcement notice.

6.3 Enforcement action

We have issued an enforcement notice to Experian about its data broking activities.

This notice requires Experian to take steps to remedy the non-compliant processing we identified through our assessment notice, which it has not already proactively addressed.

In summary, the notice requires Experian to:

- make improvements to the privacy notice on its website;

- cease the use of data provided to Experian for credit referencing purposes for any direct marketing purposes, except where requested by the individual;
- delete data supplied on the basis of consent, which is processed by Experian on the basis of their legitimate interests;
- directly provide to individuals an Article 14-compliant privacy notice, where Experian has obtained their data from a source other than the data subject (with some limited exceptions). Experian must also cease processing the personal data of any data subject it has not sent a notice to;
- cease processing personal data where an objective legitimate interest assessment cannot be said to favour the interests of Experian over the rights of the data subject (having particular regard to transparency, and the intrusive nature of profiling);
- review the privacy notices and consent mechanisms of its data suppliers for GDPR compliance; and
- cease processing any personal data where there is insufficient evidence it was collected in a compliant manner.

Experian has the right to appeal this notice to the First-Tier Tribunal (Information Rights).

6.4 Stakeholder engagement

Throughout the regulatory process, we have engaged with the CRAs and other regulators to ensure we fully understood the impact of our proposed action. We recognise the strategic significance of the CRAs to the UK economy and therefore have looked to minimise the risk of any unforeseen consequences of regulatory action. This has become especially important in light of the impact of Covid-19.

We have worked closely with the Financial Conduct Authority (FCA) in particular to understand any regulatory overlap and to assess potential economic impact. We are very grateful for the support they have provided to this investigation.

7. Conclusions

The ICO recognises that data broking can be positive for businesses and individuals. Data driven services provided by third parties can provide significant value to the growth of the digital economy and help a range of organisations improve the precision and effectiveness of their services. But data driven services, and ultimately their business models, must comply with data protection law.

Our investigation found systemic data protection failings across the data broking sector. The Commissioner is concerned that non-compliance with key principles of data protection law appears to be widespread within an industry that depends on personal data.

We recognise that while some individuals may be happy to have their data bought and sold for direct marketing purposes, and for profiles and models to be built using it, others will not be. However, if individuals do not know that processing is happening, they cannot make this decision.

All individuals have the right to be informed about the processing of their personal data, and the right to object to it. Without this knowledge, individuals cannot have effective control over their personal data. Failure to proactively provide the required level of transparency effectively deprives individuals of their data protection rights.

Our action today represents a key milestone in driving change and achieving compliance in the data broking industry. However, our work is not over. The ICO remains committed to securing compliance across this sector, and we intend to carry out further investigative, engagement and educational work.

8. Next steps

8.1 Ongoing regulation

Although we have achieved improved compliance amongst the CRAs audited through this wave of regulatory action, our work in this area continues.

We are continuing to investigate the other three large data brokers and we will publish the audit summaries for each organisation and communicate any further findings once we have completed this work. As per our usual audit practice, we will conduct follow-up work with audited controllers to ensure they adhere to our recommendations and requirements.

The ICO is currently conducting a major criminal investigation into the trade of personal data which has been obtained unlawfully from the motor accident repair sector and sold on to claims management companies. Offences under consideration include section 55 of the Data Protection Act 1998, the Computer Misuse Act 1990 and conspiracy to commit both offences. We will publish details of the outcome of our investigation as appropriate. These cases highlight the importance of appropriate due diligence when purchasing personal data.

Alongside these larger-scale operations, we will continue to investigate concerns raised by members of the public about data broking and marketing.

8.2 Educating the customers of data broking services

The Commissioner has a role as an educator as well as an enforcer.

We are aware that many different organisations will have used the marketing services of data brokers or may wish to use such services. The organisations using these services must ensure that they too comply with the GDPR and DPA 2018.

We have therefore produced specific advice for the customers or users of data brokers to remind them of their obligations.

8.3 Statutory codes of practice

The DPA 2018 places an obligation on the Commissioner to produce statutory codes of practice on certain topics. Two of the codes she is required to produce have relevance to data broking – the Data sharing code and the Direct marketing code.

Data sharing is an intrinsic part of data broking, whether this is for example obtaining personal data from third parties, or selling and licensing personal data to their customers who wish to use their services.

The majority of the processing of personal data that data brokers undertake is likely to be for direct marketing purposes. The customers of data brokers in most instances want to use the personal data they obtain for their own direct marketing purposes.

In due course, we will announce when we have submitted these codes of practice to the Secretary State as per the process in the DPA 2018. They will then be laid in Parliament.

8.4 Educating the public

The Commissioner's educational function extends to empowering individuals with advice and guidance on their data protection rights and how to help themselves.

Whilst in many instances individuals may wish to receive direct marketing, some direct marketing can be seen as a nuisance. We have guidance on our website to assist individuals in exercising their rights which includes how to object to the use of their data, and we will continue to support and educate the public to help themselves and minimise unwanted direct marketing.

8.5 Online data broking

Data broking is not limited to the offline world. It also takes place online and can play a part in the advertising that individuals see on websites.

The Commissioner has been reviewing Real-Time Bidding which is underpinned by advertising technology (adtech). Within the adtech ecosystem there are organisations operating as data brokers or which source information from them or both (for example Data Management Platforms or DMPs). Our review is looking into all the various players in this ecosystem.

There is more information on our website about our work on adtech.