STEPHENSON HARWOOD

November 2020

Make the invisible visible: five key takeaways from the Experian enforcement action

As we reported in our October data protection bulletin, the Information Commissioner's Office (**ICO**) recently issued Experian Limited (**Experian**) with an enforcement notice (**Notice**) in relation to the processing of personal data for direct marketing purposes and the use of personal data from public or third party sources.

The investigation: what did the ICO look at?

The Notice follows a two-year investigation into the direct marketing activities of three credit reference agencies - Experian, Equifax and TransUnion (**CRAs**).

The CRAs act as data brokers, enhancing and enriching personal data held in vast databases of information about almost every adult within the UK and trading it for use by the CRA customers. The ICO found that all three CRAs were offering products and services that trade, enrich and enhance people's personal data without their knowledge. The processed personal data was then being utilised for direct marketing purposes by the CRAs' customers.

The investigation looked at the CRAs' offline direct marketing services only (their online services are still under review by the ICO) and did not review the CRAs' use of personal data as part of their credit referencing functions, but rather focused on their data broking services.

The Report: what did the ICO identify as the CRAs data protection failures?

The investigation culminated in an ICO report, which analyses data protection compliance within the direct marketing data broking sector (**Report**). The Report did not find that data broking is inherently incompatible with data protection law, emphasising that "*the data broking sector provides a valuable service to support organisations across the UK*". However, the Report does highlight that data broking often involves processing large amounts of personal data, which data are regularly collected for profiling purposes (including generating previously unknown information about data subjects). The ICO acknowledges that these processing activities generally occur without appropriate transparency and in a manner that goes beyond data subjects' reasonable expectations. The risk here is "invisible processing": a type of processing that is already of particular concern for the ICO.

As part of its Report, the ICO assessed and audited the three CRAs and found systemic and "*significant data protection failures at each company*".

As a result of the ICO's engagement work, Equifax and TransUnion voluntarily made significant changes to the way they handled data, ceasing to supply non-compliant products and services.

However, while Experian made changes to its practices, the ICO found that its processing of personal data in the context of its marketing services "*remains non-compliant with the data protection law*". In particular, Experian was unwilling to issue fair processing notices directly to affected data subjects and to cease using credit reference data for direct marketing purposes, on the basis that those data subjects already had the information, or alternatively that to do so would require disproportionate effort under the exemption in Article 14(5)(b) of the General Data Protection Regulation (**GDPR**).

The Notice: what does Experian have to do?

The enforcement notice gives Experian three months to:

- clarify and make improvements to its website privacy policy;
- stop using credit referencing-derived data for direct marketing purposes, except those requested by the data subject; and

- delete data processed on the legitimate interests ground if it had originally been supplied on the basis of consent.

Further, within nine months Experian must:

- directly provide a GDPR-compliant privacy notice by mail or other acceptable means of communication wherever Experian obtained data from a source other than the data subject (such as public or third party sources) - with the limited exception that it would be disproportionate for Experian to be required to notify individuals that it is processing their collected from the Open Electoral Register. If such a notice is not sent to a data subject, Experian must cease processing their data;
- cease processing personal data where data subjects' rights and freedoms override Experian's interests, based on an objective legitimate interests assessment that has particular regard to transparency and the intrusive nature of profiling;
- review the GDPR compliance of the privacy notices and consent capture mechanisms of its data suppliers; and
- cease processing any personal data where there is insufficient evidence it was collected in a compliant manner.

Since receiving the Notice, Experian has voiced its intention to appeal the conclusions of the investigation to the First Tier Tribunal (Information Rights). Nevertheless, until such an appeal is made and regardless of any potential ruling, it is worth considering the impact of the ICO's decision now.

The takeaways: what can we learn from the Report and Notice?

The Report and Notice are not only relevant to CRAs or other data brokers: they address topics that are relevant to any business that makes use of personal data from third party or publicly available sources. Specifically, the Report and Notice provide an insight into how processing for "*surprising*" purposes may be invisible to the data subjects. This is particularly relevant for processing activities that are not automatically linked to the purpose of collection of the data, such as direct marketing.

If your organisation is in that position, there are several key takeaways that may be relevant to you. You may consider documenting your actions in light of these takeaways in a data protection impact assessment (**DPIA**), which could set out your assessment of the information given to data subjects, the proper lawful basis for processing their data and the protections in place for data subjects.

1. GET CLARITY: understand which activities constitute processing for "direct marketing purposes"

The Notice makes clear that a broad range of activities constitute processing personal data for "*direct marketing purposes*". Not only does linking attributes from a modelled marketing segment to a data subject's profile qualify; but aggregating data subjects' data to provide insights about groups amounts to direct marketing too. The ICO even considers Experian's use of credit referencing data on actual or profiled wealth to remove data subjects from marketing lists to be processing for direct marketing purposes.

This broad definition of processing for direct marketing purposes is consistent with the ICO's draft Direct Marketing Code of Practice (**Code**) (the final version of which is still pending) and should therefore come as no surprise. Direct marketing purposes under the Code "*include all processing activities that lead up to, enable or support the sending of direct marketing*". The Code sets out clear examples of what might constitute direct marketing purposes, including "*data cleansing, matching or screening*". Organisations should also note that disclosing data to third parties to facilitate their own direct marketing will also constitute processing for direct marketing purposes by both the disclosing organisation and the recipient.

The Report confirms that the final version of the Code is on its way, which is likely to provide further detail on the ICO's requirements for organisations that process data for direct marketing purposes.

2. ESTABLISH LAWFULNESS: check your legal basis for processing for direct marketing purposes

Gaining clarity of which activities constitute processing for direct marketing purposes is important for establishing the legal basis on which you undertake that processing. There are two aspects to this:

- the first is emphasised in the Notice, which highlights that where personal data has been 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 direct marketing purposes will also be consent; and
- the second relates to online direct marketing activities (not covered in the Report or the Notice) - the Code emphasises that, if consent is required under the Privacy and Electronic Communications Regulations 2003 (**PECR**), then processing

personal data for direct marketing purposes is unlawful under the GDPR without consent.

It follows that consent is likely to be the appropriate legal basis for a wide range of activities connected to direct marketing, both offline and online.

The Report does not say that legitimate interests can never be relied on as the basis for processing for direct marketing purposes. In fact, where PECR does not require consent, or data has not been collected on the basis of consent, it is likely that legitimate interests may apply to subsequent processing for direct marketing purposes. The Report states that legitimate interests is likely to be the appropriate basis where data subjects would expect the relevant processing and there is minimal privacy impact, or where there is a compelling justification for the processing, which emphasises that it is not appropriate in all cases. However, those undertaking processing for direct marketing purposes relying on the basis of legitimate interests should look closely at any legitimate interests assessment (**LIA**) they have undertaken, particularly for profiling using large data sets and data matching. Where there is a risk of invisible processing, it will be particularly important to be able to justify and defend your reliance on legitimate interests as the basis for processing.

The ICO made it clear that LIAs must make an objective assessment of the applicability of legitimate interests as a legal basis for processing for direct marketing purposes. In Experian's case, where the outcome of the objective LIA did not favour Experian's interests, the ICO has required it to cease processing.

Experian has also been told to delete any data that was supplied to it in reliance on the legal basis of consent but which has since been processed using legitimate interests as the legal basis. This was because switching to legitimate interests would mislead individuals as to the degree of control they have over their data and their ability to withdraw consent. This misrepresentation would mean that an LIA must necessarily conclude that data subjects' interests override the controller's. If your revised LIA does not stand up to objective scrutiny, you too may need to cease processing certain data.

3. ALWAYS VERIFY: do your due diligence when relying on third party consents

Where the consents on which you are relying on have been obtained by a third party, such as a data broker, you need to verify those consents, making sure they cover all of the intended processing activities which you propose to undertake and meet the requirements for valid GDPR consent (i.e that it was freely given, specific, informed, unambiguous and revocable).

Although the ICO's guidance does not impose a new requirement, it serves to emphasise the real difficulties of relying on consents that have been obtained by others as the legal basis for your processing in the context of the broad definition of processing for direct marketing purposes. These difficulties arise because any consents obtained to facilitate processing for direct marketing purposes need to be detailed enough to cover the whole range of processing which will be undertaken in pursuit of the proposed direct marketing activities at a granular level, including the fact that the data may be shared with you.

It remains to be seen how big data aggregators deal with the need to obtain very granular consents to cover their all of their customers' direct marketing-related activities. If they are faced with too many tick boxes, data subjects may simply suffer from opt-in fatigue. If required consents are not obtained, it is clear that there is a risk of regulatory sanction. Furthermore, data brokers or others may be exposed to civil claims of the sort that are currently being brought against companies such as Oracle and Salesforce.

4. BE TRANSPARENT: make sure your privacy notice is sufficiently clear

The Notice emphasises that the GDPR does not prohibit the use of publicly available personal data (whether published by the data subject or in official records) for commercial purposes, nor is the use of data supplied by third parties prohibited.

However, where the use of publicly available or third party-derived data is of an unexpected scale or scope, including for analytics or profiling, then it is particularly important to make sure that affected data subjects have a proper understanding of how you use their data such that they can effectively exercise their rights. This means setting out exactly how you use data in your privacy notice, particularly in relation to any surprising processing and in relation to the broad range of activities that constitute processing for direct marketing purposes.

It may assist your review to take into account the steps that the ICO advised Experian to take in relation to its privacy notice, which included:

- adding an "at a glance" summary of its direct marketing processing, setting out what actual and modelled attributes Experian processes about data subjects;

- ensuring that unusual or surprising processing of information appears more prominently than in the third or fourth layer of the privacy policy – this may include specifying potential uses of information for unexpected purposes, or where someone is being profiled on the sole basis of their email address;
- using clearer, everyday language (avoiding marketing terms such as "*insights*") and including intelligible information naming which public data sources are used, and to whom data might be sold; and
- giving illustrative examples and possible outcomes for data subjects, including explaining any possible drawbacks of the data broking activities.

5. BRING FAIR PROCESSING INFORMATION TO ATTENTION: make sure data subjects have the required information about the processing

Where you process personal data supplied by third parties, you may have considered relying on the exemption that the data subjects already have the relevant fair processing information, on the basis that the third party has already supplied it in its own privacy policy (Article 14(5)(a), GDPR). In relation to publicly available personal data, the disproportionate effort exemption in Article 14(5)(b) of the GDPR is also often applied.

However, the Notice emphasises that there are common circumstances in which these exemptions should not be applied. Experian has been ordered to provide a GDPR-compliant privacy notice directly to data subjects wherever it obtained data from a source other than the data subject, or to otherwise cease processing that person's data. Experian can provide their privacy notice either by mail or other acceptable means of communication but an advertising campaign would not be sufficient.

The ICO made it clear that Experian could not rely on third parties' privacy policies bringing all the necessary fair processing information to data subjects' attention. Significant, impactful and unexpected processing such as profiling and processing for direct marketing purposes by the CRAs should be actively brought to data subjects' attention by CRAs themselves. Despite this requirement to provide their own privacy policy, Experian is also required to audit its third party suppliers' privacy notices to check that they are sufficiently clear and transparent, particularly in relation to any "surprising" processing.

It was not held to be appropriate for Experian to rely on disproportionate effort either, due to the extensive and largely invisible nature of the processing (particularly the combining of public and non-public data to create marketing profiles). It follows that in most instances it would be difficult to justify relying on disproportionate effort, given that Experian's own business model means it collects and processes large amounts of data itself.

Therefore, if you are relying on your suppliers of personal data to give data subjects sufficient fair processing information, or you are relying on the disproportionate effort exemption, we advise you to give careful consideration to whether you can still justify this in your circumstances in light of the Notice. You should also carry out regular reviews of any third party privacy notices on which you rely to meet your own transparency obligations.

If your processing activities are in any way surprising, you may need to do more to bring them to data subjects' attention, including by actively sending privacy notices rather than relying on a public statement on your website.

Looking to the future

The ICO's review of the data broking sector continues, and it has said that it intends to carry out "*further investigative, engagement and educational work*" to ensure that data brokers' activities comply with data protection law. The ICO has also published guidance for organisations on making use of data brokers' marketing services, which covers lawful bases, due diligence on data brokers and transparent processing.

It is notable that the ICO chose to issue Experian an enforcement notice, rather than a monetary penalty notice, as it has recently issued in a number of high profile cases (e.g. to British Airways, Marriott and Ticketmaster), on the basis that "*this is the most effective and proportionate way to achieve compliance in this case, whilst still having a dissuasive and informative impact*". This perhaps reflects a view on the ICO's part that concerns regarding systemic processing issues are best addressed via enforcement notices, by contrast to security breaches, which it considers to be better addressed by fines. Of course, in Experian's case, subject to the Notice being upheld on appeal, the cost of complying with the enforcement notice may well significantly outweigh any fine it may otherwise have received, and may fundamentally challenge its operating model.

Clearly, the ICO wishes to engage with the data broking sector in order to bring about "*fundamental changes*" to its personal data processing practices. Accordingly, those who provide data broking

services, or who use personal data received from data brokers, should therefore review their activities and keep them under review as the ICO's work continues.

The Notice has highlighted the importance of ensuring transparency and lawfulness when processing personal data for the purpose of offline direct marketing in all sectors, not just data broking.

Now, as the ICO's related investigation into the digital advertising ad-tech sector progresses and when the final version of the direct marketing Code is laid before Parliament, it is likely that we will see more detailed guidance on how these same issues of transparency and lawfulness in data broking apply to the online direct marketing space.

Key contacts

Katie Hewson
Senior Associate
T: +44 20 7809 2374
E: katie.hewson@shlegal.com

Ben Sigler
Partner
T: +44 20 7809 2919
E: ben.sigler@shlegal.com

STEPHENSON HARWOOD