# Wealth Screening & Data Cleaning – what you need to know

BUFFALO

A DIVISION OF RUFFALO NOEL LEVITZ

## Introduction

In December 2016 and April 2017, the Information Commissioner's Office (ICO) issued fines to several charities after concluding that they had failed to comply with the Data Protection Act when conducting wealth screening and data cleaning activities.

Because of this action, many people are now asking '**Can we still do wealth screening and data cleaning?**'

This paper answers this question.

## What has changed?

Nothing. The law surrounding the protection of personal data **has not changed**. Prospect research techniques such as Data Cleaning and Wealth Screening **are not** and **have never been illegal**.

## Why were those charities fined?

The ICO found that these charities had breached one or more of the eight data protection principles contained within the Data Protection Act (DPA) when conducting their data cleaning and wealth screening activities. More specifically, there were three areas of failure:

### 1. Data Sharing – a lack of consent

Some of the charities were part of a scheme called 'Reciprocate' where they could share or swap personal data with other charities to get details of prospective donors.

The ICO ruled that the charities had not provided their supporters with enough information to allow them to make a decision on whether or not to opt out of this scheme.

**"The law surrounding the protection of personal data has not changed. Prospect research techniques such as data cleaning and wealth screening are not and have never been illegal."**

### 2. Wealth Screening – unfair processing

The charities employed wealth management companies to analyse the financial status of supporters to estimate how much more money they might be able to give. The wealth management companies also used other information from publicly-available sources to investigate income, property values, lifestyle and even friendship circles.

The ICO ruled that the processing of this data was unfair and therefore breached the first DPA principle since individuals were not adequately informed on how their personal data would be used for the purpose of wealth screening.

### 3. Data Cleaning and Tele-matching – unfair processing

Where contact information was not available, the charities hired companies to find it. For example, the companies used an old phone number to trace a new one, or used an email address to track down a postal address.

The process of trying to obtain items of personal information – which individuals have not already provided – was again deemed to breach the first DPA principle, namely it was unfair data processing.

## Can we do wealth screening?

Wealth screening is not illegal, but you must abide by the eight DPA principles. The ICO's guidance is clear:

*"The DPA doesn't stop you getting and using information from publicly available sources. However, you need to ensure that the way you do it complies with all the DPA's requirements."*

The first two principles are particularly relevant; the key issues are lawfulness, fairness and transparency:

1. **Lawfulness:** You need to decide whether you are using legitimate interests or consent as your basis for processing personal data.

   **Legitimate Interests:** is a condition by which an organisation can process personal data on the basis of having legitimate reasons for doing so, having taken account of the privacy rights and expectations of those whose personal data you are processing. This can form the legal basis for processing data without the individual's consent. You should take legal advice on whether you are comfortable using this condition in order to wealth screen, as the ICO notes there is risk in relying on legitimate interests to legitimise the most intrusive type of screening.

   **"Wealth screening is not illegal, but you must abide by the eight DPA principles."**

   **Consent:** is required if you cannot use legitimate interests as your basis for processing personal data. To be valid, consent must be knowingly and freely given, clear and specific. It must cover the type of communication you wish to use and involve some form of positive action – for example, ticking a box. The person must fully understand that they are giving you consent and you in turn must keep clear records of what individuals have consented too, when and how the consent was obtained, so that you can demonstrate compliance in the event of a complaint.

2. **Fairness:** The ICO is clear that the reasonable expectations of the individual subject to screening should be part of the assessment of whether you believe you are processing their personal data fairly. This assessment is separate from the requirement to be transparent with individuals (see below).

   When obtaining and intending to use publicly available personal information – either yourself, or via a third party – you must compare the original purpose for which it was collected and used against the purpose for which you intend to use it. The ICO is clear: *the purposes for which you intend to process the personal information must be compatible with the purposes for which its processing was originally intended.*

3. **Transparency:** You must be confident that the individual being screened would expect you to use their personal data for this purpose. The most common way of tackling this is through the use of Privacy Notices at the time the personal data is collected, supported by more detailed information in a Privacy Policy.

   A Privacy Notice is a statement made by an organisation to individuals, which discloses how it gathers, uses, discloses, and manages the individual's data.

   Note: if your Privacy Notices are being updated retrospectively, you will need to have proof that anyone who had not seen, but whose personal data has been wealth screened, is provided with the updated Notice.

The ICO is clear: "*if it would be relatively easy for you to inform individuals, you should **always do it**, even if the effect of the processing on them would not be that great…if you have individuals' data and it's feasible to give them a privacy notice – because you have lists of their names and addresses, for example – then you should do so.*"

## Can we do data cleaning?

Again, data cleaning is not illegal and in some instances, you must conduct data cleaning to comply with the DPA. However, the term 'data cleaning' is an unhelpful one and instead you should think of data cleaning as three separate methods, and analyse the level of risk for each of them. The key issue is whether you are being fair to the individual – i.e. there is a difference between

- **Data Validation** – *e.g. confirming if a phone number is still valid*
  This should be regularly conducted so that you comply with the fourth DPA principle: 'Personal data shall be accurate and, where necessary kept up to date'

- **Direct Data Enrichment** – *directly from source e.g. a customer survey*
  Methods that rely on contacting the individual ensure they continue to have choice about the personal information you hold on them. This should therefore carry minimal risk, provided you use suitable privacy notices when collecting this data, as it will have been captured fairly and therefore can be used lawfully.

- **Third Party Data Enrichment** – *via a third party e.g. BT OSIS, Royal Mail etc.*
  Obtaining personal information about the individual from other sources will reduce (or in some cases, remove) their choice about what personal information you hold about them. This will therefore pose a medium to elevated risk, depending on the sources used. Credible sources such as BT OSIS (new phones) and Royal Mail NCOA (new addresses) would carry lower risk as the person has given permission for these details to be passed on to organizations who currently hold their old details. However, other less-reputable

**"Data cleaning is not illegal and in some instances, you must conduct data cleaning to comply with the DPA."**

sources, such as lifestyle questionnaires, will be riskier since they capture personal data that an individual might not expect you to use and so it may not be deemed fair processing.

In summary, Data Validation and Direct Data Enrichment can and should continue as before, but you should ensure you are using suitable privacy notices. Third Party Data Enrichment needs more consideration on DPA compliance before being conducted.

## Does all this change again with the introduction of GDPR in May 2018?

The GDPR brings with it some additional requirements and these need to be considered to avoid duplication of effort. For example, the GDPR will require your Privacy Notices to explain your legal basis for processing the data and your data retention periods. The ICO has a paper on Preparing for the GDPR.

# How can Buffalo help?

### Data Validation

Buffalo has a range of data validation services, as listed below. These services carry minimal risk and should be regular conducted to comply with principle 4 of the DPA.

| Service | Risk Level (with no consent) |
|---|---|
| PAF | Minimal risk |
| Flagging Goneaways | Minimal risk |
| Email Validation | Minimal risk |
| De-duplication | Minimal risk |
| Active Line Testing | Minimal risk |
| TPS Screening | Minimal risk |
| MPS Screening | Minimal risk |

### Direct Data Enrichment

Buffalo has been providing its PIF (Personal Information Form) Direct Data Enrichment service to clients for many years. We have also recently worked with a company called Protecture (data protection specialists) to ensure that we have suitable template Privacy Notices that can be used by our clients when new personal data is captured.

| Service | Risk Level (with no consent) |
|---|---|
| Electronic PIF | Minimal risk |
| Paper PIF | Minimal risk |

## Third Party Data Enrichment

Buffalo only use credible third party suppliers and we can help guide you on the risk management strategy you might wish to take for this service.

| Service | Risk Level (with no consent) |
|---|---|
| Lost Alumni | Elevated risk |
| Email Append | Elevated risk |
| Mobile append | Elevated risk |
| US Data Enrichment | Medium risk |
| Telephone Number Append without XD Flags (BT OSIS only) | Medium risk |
| Mover (New Found address) (NCOA only) | Medium risk |

## Wealth Screening

Buffalo works in partnership with Prospecting for Gold, who specialize in identifying high net worth prospective donor prospects.

| Service | Risk Level (with no consent) |
|---|---|
| Wealth Tag Report | Elevated risk |
| Snapshot Report | Elevated risk |
| Million Pound Property | Elevated risk |

**For more information on these services, please contact us at marketing@buffalofc.co.uk or call the office on 01179 33 55 80.**