Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
T. 0303 123 1113 F. 01625 524510
www.ico.org.uk

[ADDRESS]

[DATE]

Dear [INSERT NAME]

Thank you for your response to our enquiries in relation to university wealth screening and data matching practices for fundraising purposes. We have now collated and analysed the responses we received, and I am writing to inform you that the ICO does not intend to take any further action in relation to this enquiry at this stage.

As you will be aware, the EU-wide General Data Protection Regulation (GDPR) has applied since 25 May 2018. The GDPR forms part of the data protection regime in the UK, together with the new Data Protection Act 2018 (DPA 2018).

The purpose of the rest of this letter is to set out the ICO's concerns about wealth screening and data matching from a data protection perspective, and to explain the facts your institution must consider to ensure you are compliant with the new laws when engaged in fundraising activities.

Wealth screening

Wealth screening is a process by which an organisation uses the personal data it has obtained to identify high profile and wealthy individuals on its database. The organisation might then go on to purchase further detail about those individuals to get an idea of their financial status. Wealth screening can also be used to 'score' individuals for propensity and capacity to begin to donate or increase donations currently made.

Wealth screening raises privacy concerns because it is the kind of processing that individuals are unlikely to expect as a result of providing their personal data to a university, even where this data is given for the purposes of fundraising. Even when individuals make a charitable donation, they would not reasonably expect the organisation to profile their wealth to see whether they are likely to increase their donations or leave a legacy donation.

This means that if you have collected data from individuals for one purpose, such as monitoring alumni employment patterns or administering donations, using that data for the purposes of wealth screening or profiling them for their potential to make future large donations is likely to be incompatible with your original purpose. It would thus be unfair, and a breach of transparency obligations, to

use people's personal data for wealth screening purposes, or to share their data with other prospect research organisations, without informing them you are going to do this.

Data matching

Data matching involves obtaining personal data from other sources which individuals did not give you when you initially collected their personal information, and appending it to the data you already hold about them.

Regardless of where you get this information, unless you return to the data subject and obtain it from them, this type of processing will be unfair in most cases. This is likely be true no matter how clearly you explain it to them, because it removes the data subject's choice about what information you hold about them. Individuals may have deliberately withheld certain information from you, such as email addresses and phone numbers, because they don't want to receive communications via these channels. By getting that information from other sources, you'll be going directly against their wishes. Individuals wouldn't reasonably expect you to contact them using details they never gave you.

What the law says

The GDPR requires organisations to process personal data lawfully, fairly and in a transparent manner. Lawfulness requires you to identify an appropriate lawful basis for your processing of personal data, and not to use that data unlawfully. Fairness means considering how the processing may affect the individuals concerned, justifying any adverse impact, and only using people's data in ways they would reasonably expect. Transparency involves being honest and open with individuals about how you are using their data, and providing them with information about what you are doing with their data, including who you are sharing it with.

There are six possible lawful bases for processing personal data. Organisations must identify a valid lawful basis for their processing before they begin. Although universities are considered public authorities, it is unlikely that fundraising from alumni forms part of your public task, and thus processing for this purpose is unlikely to be able to rely upon the processing being necessary for the performance of a task carried out in the public interest. Wealth screening is a separate and distinct activity that requires its own lawful basis for processing.

Therefore, it seems likely that for the purposes of their fundraising processing, universities will have to rely on either consent, or that the processing is necessary for the purposes of pursuing legitimate interests.

If you are relying on consent as the lawful basis for your fundraising related data processing, it is essential that you give individuals real choice and control about what you do with their data. Consent must be through a positive 'opt-in', rather than requiring people to opt out, and must be specific and granular; that is, separate consent must be obtained for each purpose for which you are using people's data. So if you want to rely on consent to use people's personal data for wealth screening activities, you need to explain clearly exactly what you want to do with the data, including who it involves sharing the data with, and obtain their consent for this specific activity. You also need to make it as easy to withdraw consent as it was to give it, and to act on withdrawals of consent as soon as you can. If you cannot get consent, or you get it but it is later withdrawn, you cannot then choose another lawful basis to rely on.

The other possible lawful basis for university fundraising activities is that the processing is necessary for the purposes of pursuing legitimate interests. If you are relying on this basis, it is essential that your processing passes the three part legitimate interests test.
This requires you to:

(1) identify the legitimate interest you are pursuing. The legitimate interests can be your own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits;
(2) show that the data processing you propose to carry out is necessary for pursuing that legitimate interests. If you can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply; and
(3) balance your interest against the individual's interests, rights and freedoms. If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override your legitimate interests.

You should keep a record of your legitimate interests assessment to help you demonstrate compliance if required.

Wealth screening may cover a broad spectrum of activities. These could range from simply segmenting your donor database by postcode, through to using dedicated third-party companies to obtain more personal information and generate donor profiles. Given the broad range of activities wealth screening can include and the different levels of intrusion they represent, the legitimate interest condition is unlikely to cover all the activities that may be considered wealth screening.

Activities such as segmenting databases by reference to postcodes or other information you already have may represent a relatively low level of intrusion into privacy. In these cases, the legitimate interest condition may be a valid basis for processing. Far more intrusive are activities such as profiling individuals, particularly where this involves getting more information that the individual has not given you, either directly or via third-party companies. In these cases the legitimate interest condition is unlikely to apply. So you'd need to seek the consent of individuals before doing such processing. It follows that there is an element of risk in relying on the legitimate interest condition for wealth screening. For more certainty you should seek the individual's consent.

Processing people's data fairly means that you should only handle personal data in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them. Assessing whether you are processing information fairly depends partly on how you obtain it. In particular, if anyone is deceived or misled when the personal data is obtained, then this is unlikely to be fair. Failing to specify wealth screening as a purpose for processing would likely be considered unfair.

Transparency is fundamentally linked to fairness. Transparent processing is about being clear, open and honest with people from the start about who you are, and how and why you plan to use their personal data.

Individuals have the right to be informed about the collection and use of their personal data. You must provide individuals with information including your purposes for processing their personal data, your retention periods for that personal data, and who it will be shared with. You must provide privacy information to individuals at the time you collect their personal data from them. If you obtain personal data from other sources, you must provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month.

Transparency is important even when you have no direct relationship with the individual and collect their personal data from another source. In some cases, it can be even more important - as individuals may have no idea that you are collecting and using their personal data, and this affects their ability to assert their rights over their data.

If the university is to continue or begin processing of this nature it would be advisable to consider whether it is appropriate to conduct a Data Protection Impact Assessment (DPIA). A DPIA is a process to help you identify and minimise

the data protection risks of a project. A DPIA should describe the nature, scope, context and purposes of the processing; assess necessity, proportionality and compliance measures; identify and assess risks to individuals; and identify any additional measures to mitigate those risks. You should consult your data protection officer and, where appropriate, individuals and relevant experts. Any processors may also need to assist you. If you identify a high risk that you cannot mitigate, you must consult the ICO before starting the processing.

The ICO has published guidance on lawful bases for processing, including legitimate interests, consent and other relevant topics including the right to be informed, and DPIAs, which can all be found in the Guide to the GDPR, in the following link:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

In addition the Institute of Fundraising has also published relevant guidance:
https://www.institute-of-fundraising.org.uk/guidance/key-iof-guidance/understanding-gdpr/spotlight-series/

The ICO expects that any processing for the purposes set out above takes our guidance and advice into account. If we receive complaints in the future, any subsequent enquiries we make may lead to formal enforcement action.

Yours sincerely

Victoria Cetinkaya
Senior Policy Officer