Due Diligence Questions to ask Data Suppliers

Introduction

GDPR requires data controllers to be able to 'demonstrate that processing is in accordance with this Regulation'. This is a high bar of proof, and you are jointly liable for an infringement of the law unless you prove otherwise. If you source direct marketing data from third parties, you need to make sure they comply with the Regulation, otherwise you will not have the proof you need to show your innocence.

You should look for answers which are consistent with other information you have about the supplier. It goes without saying, you should only use suppliers who answer satisfactorily.

Here is a non-exhaustive list of questions you should be asking prospective data suppliers.

About the Organisation

What is your ICO Registration Number?

Any reputable data company will be registered with the ICO. Check with the ICO website to ensure the registration details agree with the organisation you are talking with.

What is your Company Registration Number?

Not all companies are registered with Companies House, but most will be. You should assure yourself the organisation is not a scam, and has a real world presence, and that those details agree with the company you are talking with.

What is your web address?

Look at the website and check the address details agree with other details above.

How many records are available in your data?

How frequently do you update the data?

How do you update the information?

How many people does the company employ?

Taken together these questions tell you about the plausibility of claims and the scale of the organisation. An organisation with 1 million records, which it updates annually by telephone would need in the order of 50 calling staff.

GDPR states personal data should be kept accurate, so you also need to be confident about the method delivering accurate data.

About the Data Collection Process

Was all the processing done in the EU?

GDPR sets standards for personal data protection concerning data subjects in the EU. If data is processed outside the EU, you should be vigilant about the organisation. Perhaps they have not complied with GDPR, and you could be jointly liable.

What legal basis did you use to process the data?

All data processing must have a specified legal basis. In this case you might expect either 'consent' or 'legitimate interest' to be used.

If consent, Was my organisation named when the data was collected?

For consent to be valid, **your** organisation must be named at the point of collection.

What script was used to collect the data?

You need to check the data subject was informed of how their personal data would be used, and that it will be used for direct marketing.

Was all data collected using this script or form?

You should check for different versions of scripts and forms, to ensure all the data complies, earlier versions of scripts might not comply.

If No, Please supply earlier versions of scripts and dates they were active

About Keeping the data Accurate

How will you notify me of data subjects who object to direct marketing?

GDPR requires controllers to notify recipients of the data, such as people who ask not to be marketed to.

How will you notify me of changes to the data?

One of the principles of GDPR is accuracy and it requires controllers to notify you about changes and updates to the data.

How frequently will I receive updates?

You should expect to have updates to data at least monthly.

Samples

Ask for a sample of records, but ones **you** choose, maybe even ones you know, so they are not a 'golden sample'.