Paul Evans Associates

unlocking the power of your data

Guide to Data Acquisition in a GDPR age

Part A: Questions to ask your data supplier prior to leasing b2b data

1. What is the process & methodology of data capture and maintenance?
2. What is the accuracy and recency of the data i.e. update cycle, average data age, oldest possible record?
3. What deliverability guarantees or refund policy is in place?
4. Does the refund policy account for hard bounces?
5. What is the legal basis for offering the data i.e. 'Consent' or 'Legitimate Interest'?
6. If Consent, you need to understand the specific context in which the consent was sourced as GDPR dictates that Consent needs to be by named account i.e. a list owner will need to be able to demonstrate that their data subjects have specifically consented (by channel) to receive communications via; mail, telemarketing and email marketing from the Licensee i.e. the company who will be using the data.
7. Are you fully aware of the terms of use of the data and the consequences of any unauthorised use?
8. Best practise dictates that you test some sample records.

Part B: Data Processor Agreement

1. If you are transferring Personal Information from a Data Controller to a Data Processor, then the Data Controller must get a signed Data Processor Agreement in place PRIOR to the Personal Information being released. This is an essential aspect of the GDPR. In addition to the main clauses that need to appear in this agreement, specific reference needs to account for the required services of the Data Processor. These services should appear as a schedule to the Data Processing Agreement and should include:
   a. written instructions concerning the nature & purpose of the processing;
   b. details of the types of data and categories of data to be processed;
   c. duration of the project;
   d. details of data deletion / disposal once the project is completed.
2. Data should not be transferred outside the European Economic Area without the written permission of the Data Controller and if permission is forthcoming, all parties must ensure an adequate level of protection to any Personal Information equivalent to the requirements imposed under the GDPR.
3. The Data Controller must be made aware and grant permission prior to a Data Processor being able to forward your Personal Information to a Sub-Processor or Third Party (i.e. a list owner).
4. Any Sub-Processor / Third Party MUST be signed up to the equivalent terms so as to ensure the security of your Personal Information.
5. The agreement needs to account for the obligations of the Data Processor including but not limited to: organisational and technical security measures; record keeping of the data processing; demonstration of compliance; subject access requests (where relevant); data subject complaints, the confidentiality of staff who have a need to use or process your Personalised Information and the deletion/disposal of the data after the data processing has been completed.
6. The agreement needs to highlight the relevant indemnity and liability for any unauthorised or unlawful processing, accidental loss, destruction, damage, alteration, or disclosure.

7. All Personal Information (including suppression files) MUST be transferred using suitable technical security measures i.e. data encryption. Transferring data via email attachments is not permitted under GDPR.
8. We would recommend that Data Controllers seek clarification of safe receipt of your Personal Information by a Data Processor and cross check volumes to ensure that Personal Information has not become corrupted during transfer.
9. It is also recommended that your Personal Information is inclusive of dummy/seed name(s) so as to assist you in detecting any unauthorised use of your data asset.
10. Assuming a 12-month data lease, we would recommend you seeking clarification of what GDPR update mechanisms are in place, whether these updates are optional or mandatory and what is the frequency of any updates i.e. fortnightly, monthly or quarterly updates?
11. Please do bear in mind the increased burden of updating data on a fortnightly basis versus the burden of updating data quarterly.
12. Is the update part of a refresh of the original order? If so, does the refresh account for the same data or the same selection criteria i.e. potentially inclusive of net new names? Can the list owner differentiate the records so as to assist the Licensee to easily determine changed/amended records from deleted records and net new records?
13. Finally, please note that outright purchase of prospect data base in the European Economic Area should not by possible as GDPR does not permit for data to be processed and stored indefinitely without some means of keeping it refreshed and updated.

Part C: Prior to Use of the Prospecting Data

1. Upon receipt of any prospecting data, we would urge the Licensee to delete any fields of data that are not required in support your campaign. This is in line with the 'Data Minimisation Principal' of the GDPR.
2. If you are using prospecting data under the legal grounds of 'Legitimate Interest', then the Licensee needs to have conducted a Legitimate Interests Assessment whereby you've defined the purpose of data processing and have balanced the needs of the business with the rights and fundamental freedoms of the data subjects. This should form part of your record keeping process by way of conforming to the 'Accountability Principal' of the GDPR.
3. All Data Subjects have the 'Right to be Informed' whereby at the first point of contact/communication, they are made aware of the following:
   a. Data source
   b. What personal information is held
   c. Purpose of use & legal grounds for use
   d. Rights of the data subject
   e. How long the data will be retained
   f. Data subjects should also be referred to your privacy policy / notice

   If your first communication is via email, this information should appear within the footer.

Part D: Summary of prospecting via B2B marketing in the UK

Channel to Market	Governing Legislation	Legal Status	Requirements
Direct Mail	GDPR (the General Data Protection Regulation)	Opt-out	Screen against your in-house suppression file
Telemarketing	PECR (Privacy & Electronic Communications (EC Directive Regulations 2003	Opt-out	Screen against your in-house suppression file & screen against TPS / CTPS
Email Marketing	PECR (as above)	Opt-out	Screen against your in-house suppression file, remove all non-corporate subscribers i.e. sole traders and partnerships (unless in Scotland). It is therefore OK for you to conduct email broadcasts to corporate subscribers i.e. Ltd, Plc, LLp, Government bodies and partnerships in Scotland subject to you adhering to best practise guidelines i.e. a simple to use unsubscribe, offer must be of a business to business nature and be relevant to the sector and role of the data subject.

NOTE: **The Privacy and Electronic Communications Regulation is due to be superseded by the ePrivacy Regulation (ePR). Whilst no date has been finalised for the introduction of this new legislation, it is not likely to be introduced until 2019 or even 2020. The current draft version of the legislation means that the UK's current opt-out position in respect of b2b email marketing is likely to revert to an opt-in status so that the UK's data protection standards are harmonised with the other EU member states, the vast majority of which already operate on the basis of an opt-in policy.**

Northwood House, Northwood, Shrewsbury, Shropshire SY4 5NN UK
Tel/Fax: +44 (0)1948 710236
E-mail: paulevans@paulevansassociates.com Web: www.paulevansassociates.com
Paul Evans Associates UK Limited Registered in England and Wales No: 11657510 VAT Registration Number 308 4995 71