GENERAL DATA PROTECTION REGULATION:

A CHECKLIST FOR ECOMMERCE AND MARKETING

VENTURE STREAM alphagraphics®

made in partnership with AlphaGraphics
design & print marketing experts

ECOMMERCE | DIGITAL MARKETING | DESIGN & DEVELOPMENT

www.venturestream.co.uk

CONTENTS

GDPR - CHECKLIST FOR ECOMMERCE AND MARKETING

On May 25th 2018, new data protection laws – specifically the EU General Data Protection Regulation (GDPR) – will come into force. Any business that engages in marketing activities will need to be aware of these regulations or risk facing heavy fines in cases of non-compliance.

Two facets of a B2C and B2B business that GDPR changes will have an impact on are:

1. Employment
2. Marketing

For the purposes of this guide, we will focus solely on GDPR compliance for businesses that collect, process and store data used for marketing. This refers to data collected from potential customers and customers during marketing-based data collection activities and at the checkout / order processing.

STEP 1: CARRY OUT A FULL AUDIT OF DATA CURRENTLY HELD WITHIN THE BUSINESS AND SHARED WITH 3RD PARTIES

Before amending policies, processes and data capture mechanisms to be GDPR compliant, take stock of what data you already collect, for what purpose and what steps you may (or may not) already take to compliantly collect, process, store and transfer data.

- Establish what data is held - across what categories (names, age, email, address, DOB, salary, average spend, purchase history - etc.)
- Where the data is held
- How this data was collected (i.e. with consent, without consent or unknown)
- Who has access to the data, including which 3rd parties have access to the data (should this access be limited to protect it and minimise the risk of a breach?)
- Are we keeping it safe and secure using a level of security appropriate to the risk? For example, will encryption or pseudonymisation be required to protect the personal data we hold?
- Are we transferring the personal data outside the EU and if so, do we have adequate protections in place?
- Do we review and audit the data we hold on a regular basis?

After establishing the above across the business and its operations, you will be in a much better position to begin reviewing current data, collection mechanisms, data collection processes and 3rd party processes.

After reviewing the articles within the GDPR legislation, we have compiled the following guide which should serve as a useful starting point on your journey to compliance.

Our guide has been split into sections, relating to working towards compliance across the following areas (but tailored specifically to marketing, omitting employment-related recommendations):

- Internal corporate governance
- Privacy notices
- Lawfulness of data processing
- Data subject rights
- Privacy by design
- Transfer of data
- Data security
- Breach notifications

DISCLAIMER

This information is not the same as legal advice. Where these changes apply to you, we strongly suggest that you consult a lawyer if you'd like advice on your interpretation of this information or its accuracy. In a nutshell, you may not rely on this paper as legal advice, nor as a recommendation of any particular legal understanding.

CORPORATE GOVERNANCE		
Statement	**What does this mean for my business?**	**Have I actioned this? (Y/N)**
Establish whether you are required to have a nominated / dedicated Data Protection Officer (DPO)	If the answer to one of the below points is yes, you may be required to have a DPO. • **Do the core activities of the business consist of processing a large scope of special categories of personal data and/or data relating to criminal convictions or offences** • **Do core activities consist of monitoring operations which, by virtue of their nature, require the regular monitoring of data subjects on a large scale**	
Establish how long it is necessary for each category / grouping of data to be held	Data can 'only be held for as long as necessary'. Decide how long within your industry / for each database is 'necessary' and establish a system to remove / destroy data when it runs over that period.	
Example: At point of purchase, you may collect a name, address and phone number to fulfil the customer order. The phone number may only be needed to call the customer should there be a delivery issue. The address on the other hand, may be needed to notify the customer about changes to the product / service they bought or need to be on-file should that product be recalled. In this case, the phone number information could be deleted after 2 months, with address information on-file for 12 months.		
Train employees that handle personal data	Employees that handle the personal data of other employees or customers must receive training to ensure that they can handle that data in accordance with GDPR changes. The company must keep a record of this training, update it and provide refresher training when needed.	

CORPORATE GOVERNANCE		
Statement	**What does this mean for my business?**	**Have I actioned this? (Y/N)**
Draft policies and procedures	As part of demonstrating that the company has considered its privacy obligations and implemented data protection principles, the company must hold data protection policies. The form these take and how many are needed is dependent on the business's activities. The following is a list of common policies: • General Data Protection Policy • Data Subject Access Rights Procedure • Data Retention Policy • Data Breach Escalation and Checklist • Processing Customer Data Policy • Guidance on Privacy Notices • Internal Processes and Procedures for handling data (these do not need to be publically available, but they should be documented)	
Train employees that handle personal data	In cases where your third party vendors are processing personal data on the company's behalf, ensure contracts with them have been updated to include those same processor requirements under the GDPR.	

Example publicly published policies, statements and notices (either in situ, or template form) for the above list can be found at the links below:

- **General Data Protection Policy**
- **Data Subject Access Rights Procedure**
- **Data Retention Policy** (this includes a list of the data collected and for how long each aspect will be retained)
- **Data Breach Escalation and Checklist**
- **Privacy Statement**
- **Privacy Notice**

PRIVACY NOTICES

Privacy notices must be given at the time data is obtained from the data subject or, if the data was received from a 3rd party, within one month of obtaining the data.

Statement	**What does this mean for my business?**	**Have I actioned this? (Y/N)**
Ensure privacy notices contain all of the required information	This includes: • The name and contact details of the data controller / data protection officer (where applicable) • The intended purpose of processing the personal data and the legal basis for the processing of that data • The recipients of that personal data (if any) • The period for which the data will be stored (or, the criteria used to determine that period) • If you intend to share with, or transfer this data to a 3rd party, this must be stated here along with how the data will be transferred to ensure mechanisms are approved data transfer mechanisms • Information about the right to request access to, ratification of or erasure of data concerning the subject • The existence of the right to withdraw to consent at any time	
Ensure privacy notes are clear	Ensure privacy notes are written in concise, transparent and plain language. An Information Commissioner's Office (ICO) guide to creating a **GDPR compliant Privacy Notice can be found here**.	

Example: Amazon.com has been GDPR compliant since 2016. View an example of the Amazon.com privacy policy here: **Amazon Privacy Notice**

LAWFULNESS OF PROCESSING		
Statement	**What does this mean for my business?**	**Have I actioned this? (Y/N)**
Establish the legal basis on which grounds it processes the data	You must confirm for any data which legal basis the business will use as grounds to process the data. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual. 'Contract' requirements will be of interest to those in ecommerce and businesses that store customer data. 'Consent' and 'Legitimate Interests' will be the grounds most commonly used by marketeers to gather information and so we have bolded this basis below. THE 6 LAWFUL GROUNDS CAN INCLUDE: 1. **The subject has consented to the collection and processing of his/her personal data** Consent requires a positive opt-in. Don't use pre-ticked boxes or any other method of default consent. Explicit consent requires a very clear and specific statement of consent. Keep your consent requests separate from other terms and conditions.	

LAWFULNESS OF PROCESSING		
Statement	**What does this mean for my business?**	**Have I actioned this? (Y/N)**
Establish the legal basis on which grounds it processes the data (cont.)	2. Processing is necessary for the fulfilment of a contract (e.g. email for delivery notifications, address for goods delivery, address for electricity / water / internet / phone line supply) 3. Processing is legally necessary / required 4. Processing is necessary to protect vital interests of subject or another natural person **5. Processing is necessary for legitimate interests pursued by controller or third party.** This is likely to be most appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing. There are three elements to the legitimate interests basis. It helps to think of this as a three-part test. You need to: • Identify a legitimate interest; • Show that the processing is necessary to achieve it; and • Balance it against the individual's interests, rights and freedoms.	

LAWFULNESS OF PROCESSING		
Statement	**What does this mean for my business?**	**Have I actioned this? (Y/N)**
Establish the legal basis on which grounds it processes the data (cont.)	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. The processing of the data must still be necessary. If you can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply. You must balance your interests against the individual's. If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override your legitimate interests. 6. Public task (not commonly applicable to businesses): Collecting data 'in the exercise of official authority'. This covers public functions and powers that are set out in law; or to perform a specific task in the public interest that is set out in law.	
Ensure that the legal basis on which you're collecting data applies to all of the categories of data that you collect	For example, is telephone number required for goods delivery or not? ('necessary for the fulfilment of the contract) The data subject must have given explicit consent for all of these categories of data.	

LAWFULNESS OF PROCESSING		
Statement	**What does this mean for my business?**	**Have I actioned this? (Y/N)**
Ensure consent is clearly and freely given and able to be withdrawn	Ensure consent is: • Freely given • Presented in clear and plain language • You must be able to demonstrate that the data subject gave their consent • Data subject must have the ability to withdraw consent	
Right to be forgotten	As well as having the right to withdraw consent, the data subject has the right to request the deletion of part or all data held relating to them. Ensure data is stored in such a way that all information on any specific data subject can be promptly removed.	
Profiling - does the company carry out profiling on customers?	If so, the profiling needs to ensure and be able to prove that it has the consent of the data subject to be profiled in this way.	

3RD PARTY DATA PROCESSORS AND INTERNATIONAL TRANSFERS		
Statement	**What does this mean for my business?**	**Have I actioned this? (Y/N)**
Written contracts with each data processor	If the business works with 3rd party data processors, there must be a written contract with each processor that includes **the minimum requirements from Article 28**. The Company must also ensure that it has received 'sufficient guarantees' from its data processors that they can implement measures (technical and organisational) to meet the requirements of the GDPR.	
Transferring data out of the European Economic Area (EEA)	If so, you must use one of the approved data transfer mechanisms. The approved transfer terms are as follows: a. A country which has a finding of adequacy from the European Commission b. If it is within the The Company group, are binding corporate rules in place? c. Standard contractual clauses as approved by the European Commission d. If the transfer is to the US, on the basis of the Privacy Shield. e. With the consent of the data subject. f. The transfer is necessary to carry out a contract with the data subject g. The transfer is in the public interest h. The transfer is necessary to establish, exercise or defend legal rights i. The transfer is necessary to protect the vital interests of a person where the data subject is physically or legally incapable of giving consent.	

SECURITY		
Statement	**What does this mean for my business?**	**Have I actioned this? (Y/N)**
Are security measures appropriate for the personal data?	Security has to be appropriate to the likely risks to individuals if data was lost, stolen or disclosed to unauthorised people. Security covers organisational (i.e. people, processes) and technical measures. The following factors should be considered: • Pseudonymisation • Encryption • Ensuring ongoing integrity, confidentiality, availability and resiliency • The ability to restore in a timely manner • Processes for testing security.	
BYOD - Bring Your Own Device	Consider the implication BYOD has on security risk. Should an employee's personal device be lost or stolen, could this put customer data at risk? **Minimise the security risk of BYOD**.	

BREACH NOTIFICATIONS		
Statement	**What does this mean for my business?**	**Have I actioned this? (Y/N)**
Report data breach within 72 hours	The business must report a breach to the regulator (the ICO) within 72 hours of becoming aware of it. The breach must be investigated and details provided to the regulator about the nature of the breach, likely consequences and mitigations being taken to address it. This investigation may require assistance from processors, so operational processes should factor this in. Be sure to refer to your **Data Breach Escalation and Checklist** in the event of a breach.	
Notify all individuals affected by a breach	Individuals must be promptly notified of the breach if there is a risk to their rights and freedoms. Note that if data is encrypted or otherwise unintelligible, then individuals will not need to be notified.	

GDPR COMPLIANT DATA COLLECTION EXAMPLES:

Many marketers will rely on the 'legitimate interests' legal basis for processing when sending direct mail.

It's important to obtain granular consent to distinguish between marketing mediums. Below, we've detailed some generic examples of compliant data collection along with in-situ examples.

Note: It's important to remember when using tick-box opt-ins, that you may be required to prove that they gave this consent. For this reason it is best to use tick-box forms alongside double-opt in processes via email to leave a proven trail of active opt-in actions.

GENERIC EXAMPLE FROM ICO GUIDANCE:

Here at [organisation name] we take your privacy seriously and will only use your personal information to administer your account and to provide the products and services you have requested from us.

However, from time to time we would like to contact you with details of other [specify products]/ [offers]/[services]/[competitions] we provide. If you consent to us contacting you for this purpose please tick to say how you would like us to contact you:

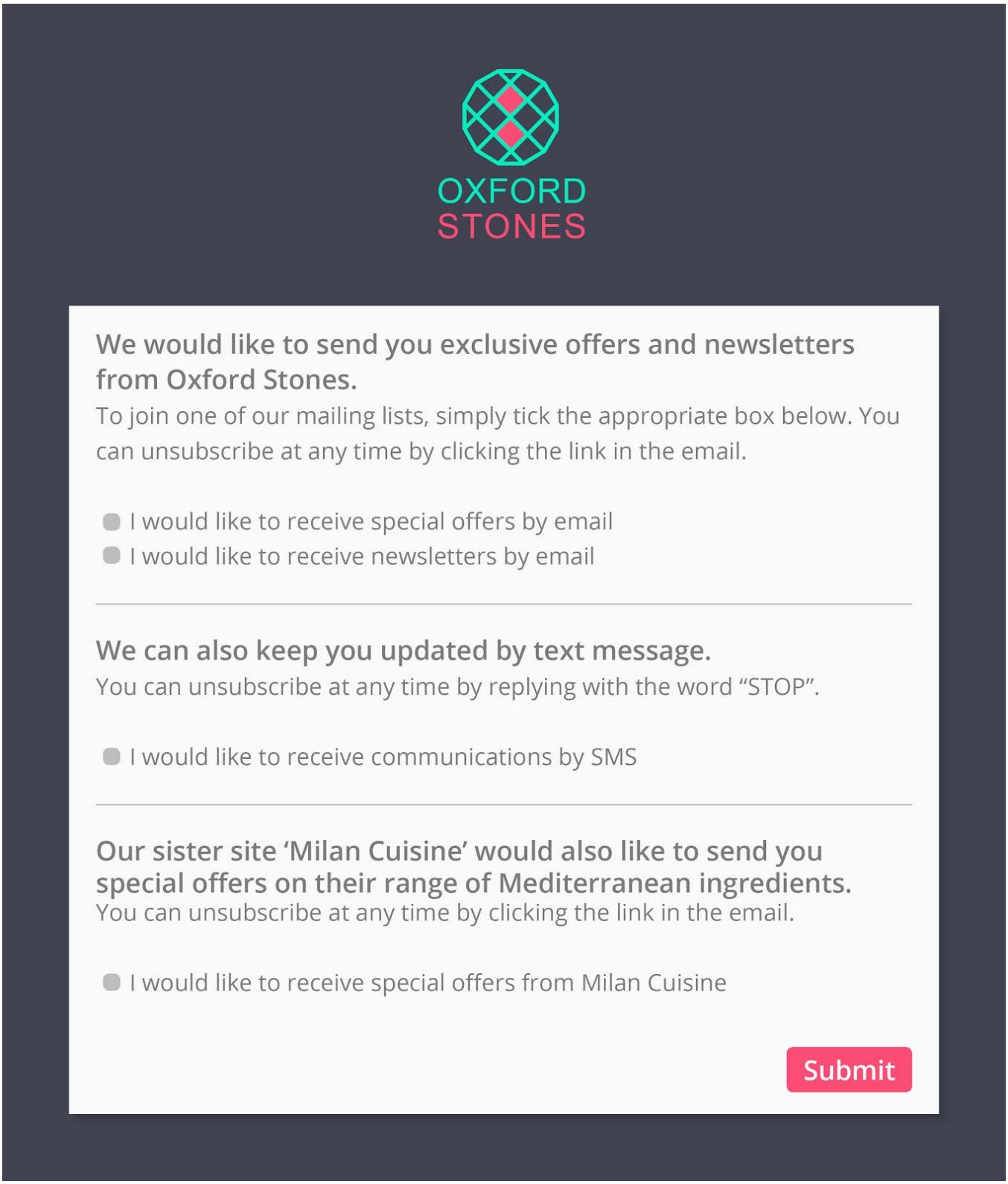
Post ☐ **Email** ☐ **Telephone** ☐

Text message ☐ **Automated call** ☐

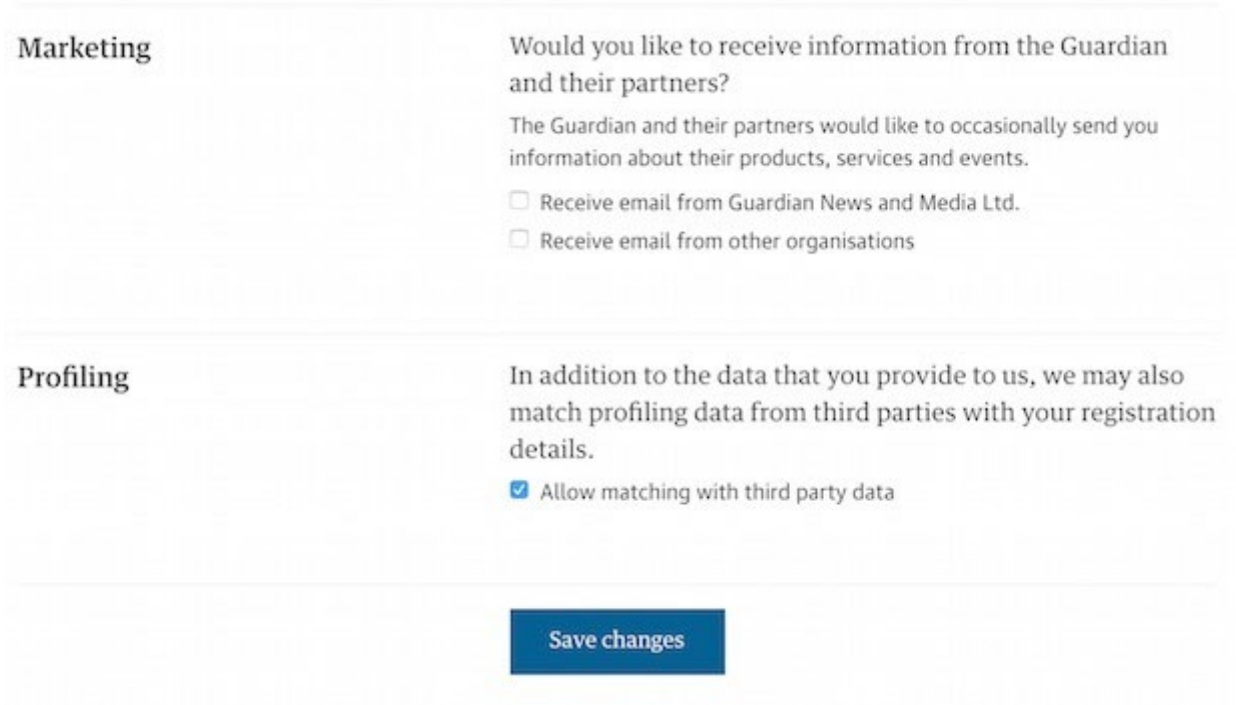
We would also like to pass your details onto other [name of company/companies who you will pass information to]/[well defined category of companies], so that they can contact you by post with details of [specify products]/ [offers]/[services]/[competitions] that they provide. If you consent to us passing on your details for that purpose please tick to confirm:

I agree ☐

OPT-IN EXAMPLE FROM OXFORD STONES (GRANULAR CONSENT)



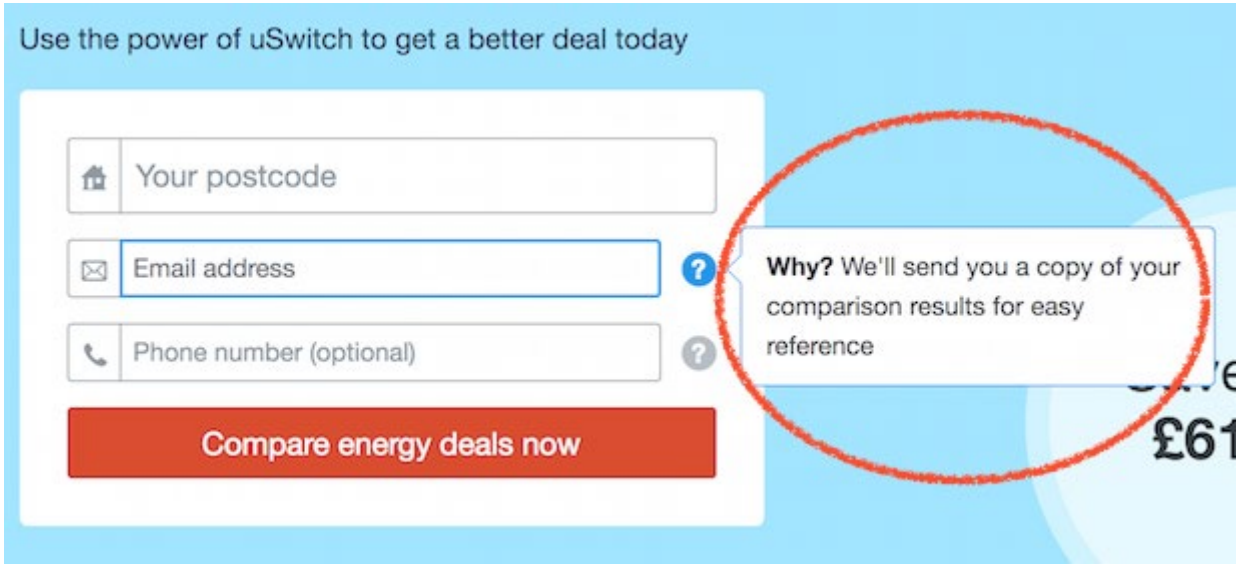
MARKETING OPT-IN AND PROFILING CONSENT EXAMPLE FROM THE GUARDIAN:

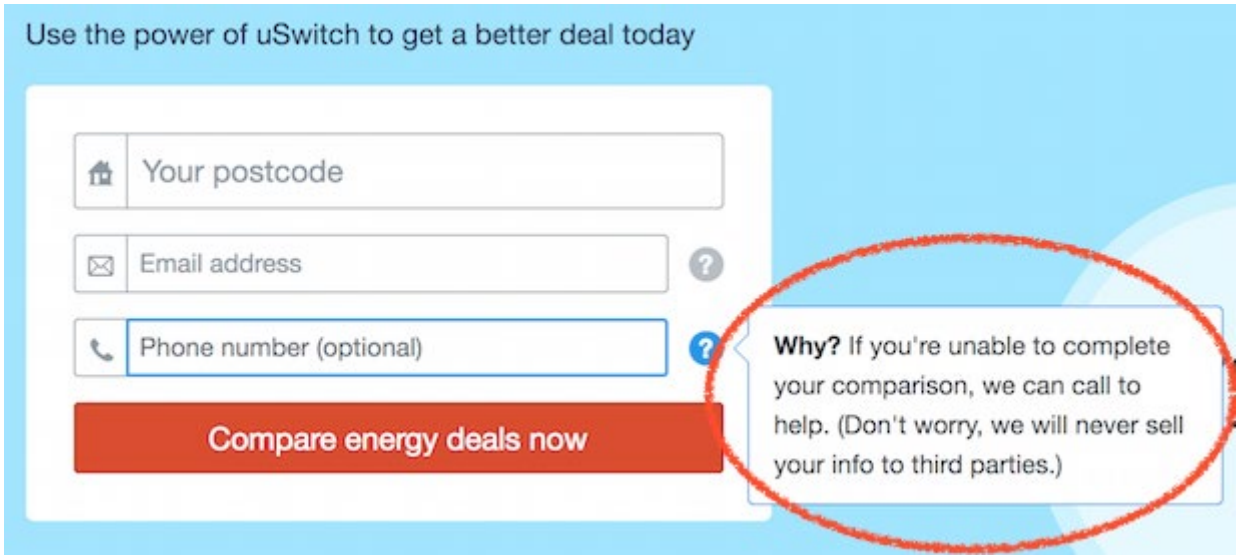


JUST-IN-TIME INFORMATION EXAMPLE FROM USWITCH:

The below example shows how pop-up, just-in-time information can be used to give clarity to the user based on the need to collect information to fulfil a service. For best-practice this example should be accompanied by a link to a privacy notice, where the person opting-in can read why the company needs the data and read more about how it will be used.

If you wish to use the information collected for marketing rather than fulfilment, then this requires explicit opt-in.





CHECKLIST FOR A COMPLIANT MARKETING OPT-IN PROCESS	
Checklist Item	**Done?**
No pre-ticked boxes. *Pre-ticked boxes do not count as consent.*	
No 'check to opt-out' boxes. *(The subject must **not** have to check a box to opt-out (i.e. the wording for consent cannot be reversed, as this could be deemed confusing))*	
Clear and concise wording. *The wording must be clear so that the data subject knows what they are opting in for and how their data will be used.*	
Separate terms and conditions and marketing opt-in boxes. *Terms and conditions and marketing consent cannot be bundled together.*	
Separate consent is required for separate forms of marketing. *Example: collect SMS and email marketing opt-in separately.*	
Name 3rd Parties. *Name any third party controllers who will rely on the consent.*	
Make withdrawing consent simple. *Make it easy for people to withdraw consent and tell them how. This information can be included in your Privacy Notice.*	
Keep evidence of consent. *Including who, when, how, and what you told people.*	
Keep consent under review. *Refresh consent information if anything changes.*	

made in partnership with AlphaGraphics
design & print marketing experts

ECOMMERCE | DIGITAL MARKETING | DESIGN & DEVELOPMENT

www.venturestream.co.uk