GDPR SIDEBAR: Best Practices for Complying with GDPR Consent Requirements

Dana B. Rosenfeld

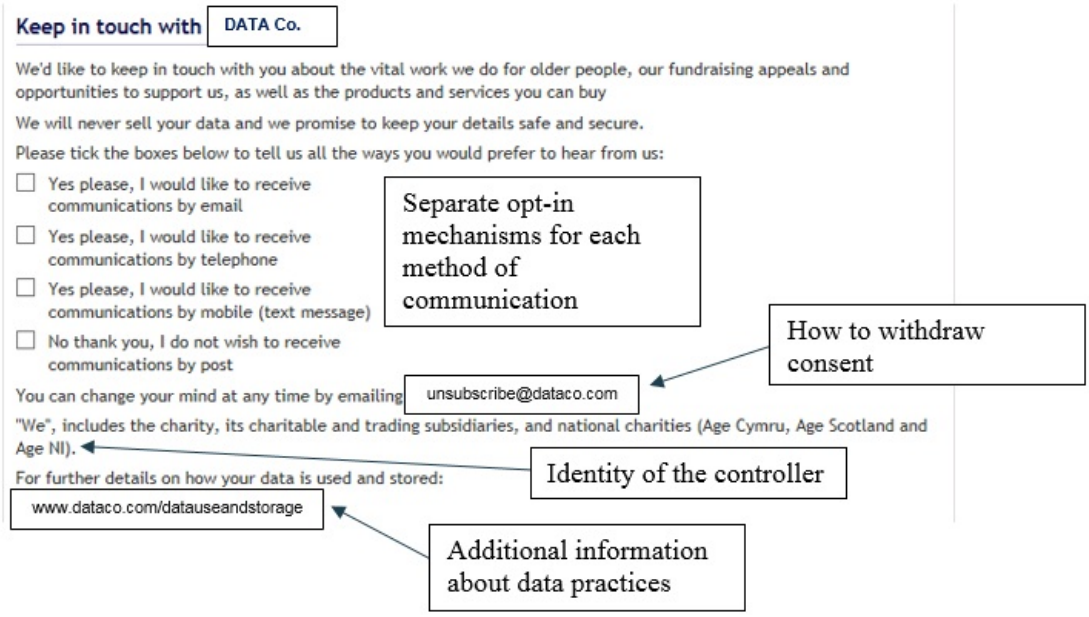
June 25, 2018

Under the GDPR, processors must have a lawful basis for processing any data of an EU data subject. Consent is one of six lawful bases[1] under the GDPR, and in this installment of GDPR SIDEBAR, we'll cover best practices that can help achieve an acceptable level of compliance with GDPR consent requirements.

Valid consent under the GDPR must be: (1) freely given; (2) specific; and (3) informed. And a consumer must make a clear, affirmative action to consent. This means pre-populated check boxes aren't going to count as valid consent for GDPR purposes. Here are a few tips for meeting GDPR's consent requirements:

- ***Make sure consent is specific.*** Identify what type of processing the data subject is consenting to, so that the data subject understands exactly what data is collected and how it is used. Example 1 provides a consent mechanism for each specific type of communication (text message, email, etc.). This makes it clear to the data subject what she is signing up for when she consents to processing.

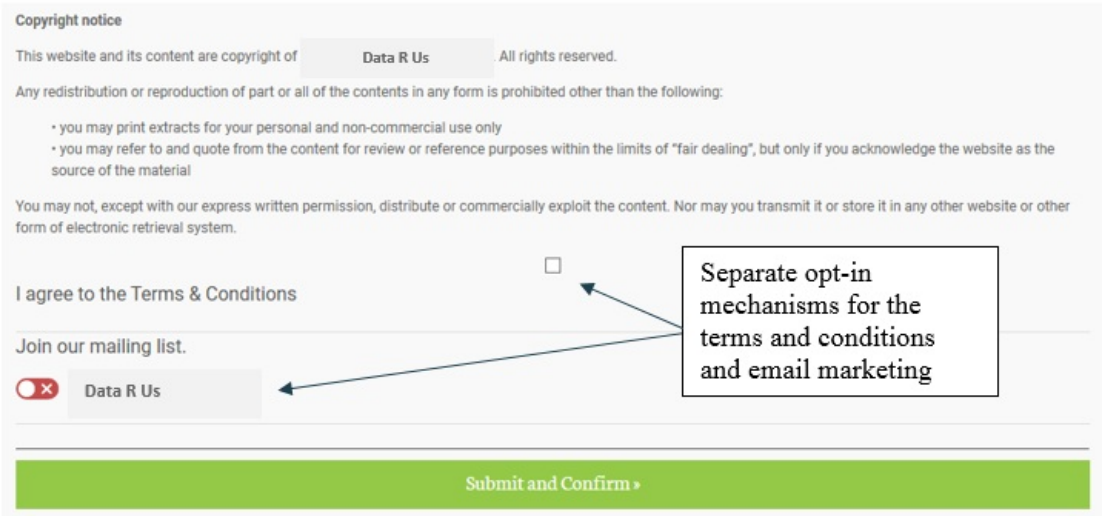
Example 1: Marketing Email Sign-Up



- ***Make sure consent is unbundled.*** Provide a separate consent mechanism for each type of

processing the data is expected to be used for. Do not bury consent in an agreement for terms and conditions or a general privacy policy. Example 2 offers unbundled options for separately consenting to marketing messages and the website's terms and conditions.

Example 2: Profile Registration



- ***Make sure to provide enough information.*** State: (1) who the controller is; (2) how the data will be used; (3) what type of data will be used; (4) that the data subject can withdraw consent; (5) how the data will be used for automated processing decisions; and (6) the possible risks associated with data transfers (if applicable). Example 1 clearly separates out each of these requirements in the consent mechanism. The additional information via a hyperlink is clearly labeled and takes the consumer directly to a page with additional information about the company's data processing.
- ***Make withdrawing consent an easy process.*** Ensure that a data subject can easily withdraw consent for processing if she so chooses. This should be a one-step process, such as clicking a button or un-checking a box. Examples 1 and 2 provide easy, single-step opt-out mechanisms. In Example 1, the data subject sends an email to the provided address. Example 2 makes it even easier, allowing the data subject to click a sliding button to opt out.
- ***Keep adequate records of data subjects' consent*.** Record how and why data subjects have given their consent to data processing. Since the controller has the responsibility to provide a record of consent, adequate records are necessary in case processing is challenged.
- ***Harmonize U.S. and EU consent requirements*.** If doing business both in the U.S. and EU Member States, it is easiest to implement consent practices that are sufficient for both countries. Trying to differentiate will likely become complicated.

Stay tuned for upcoming sidebars on additional GDPR consent requirements.

[1] The six lawful bases are the following: consent; contract; legal obligation; vital interests; public task; and legitimate interests. The Article 29 Working Party has warned that "when initiating activities that involve processing of personal data, a controller must always take time to consider what would be the appropriate lawful ground for the envisaged processing."