Privacy

No Purchase or Personal Data Collection Necessary: GDPR's Impact

Privacy Regulation

The European Union's new data privacy rules are set to take effect May 25 and will have broad implications for businesses across industries. Robert Laplaca of Verrill Dana discusses how the new rules will affect online sweepstakes, and he breaks down the requirements that contest sponsors must comply with.

By Rob Laplaca

The General Data Protection Regulation (GDPR) goes into effect May 25, with the goal of protecting European Union residents' online personal data. Sweepstakes are all about personal data collection. Sponsors use the information to create mailing lists, generate leads and, if lucky, get free marketing from user-generated content (cue up the Oscar Meyer wiener song that came from a jingle contest).

What does the GDPR mean for U.S. brands running sweepstakes open to our friends across the pond? And, maybe more importantly, is this a harbinger for stricter regulation of U.S.-based sweepstakes?

> *Rob Laplaca is an attorney at Verrill Dana LLP in Westport, Conn., focusing on advertising, marketing, and promotions, as well as business litigation. He can be contacted at rlaplaca@verrilldana.com or (203) 222-3110.*

To answer the second question first, U.S. sweepstakes operators have few data collection obligations. Essentially, inform entrants that they are subject to a lengthy and comprehensive (and incomprehensible) privacy policy, and the sponsor is good to go. Recently, however, Congress has taken an interest in online personal privacy—just ask Facebook Inc. CEO Mark Zuckerberg. And Facebook itself has announced that it would make the GDPR controls available everywhere. So, whether a sponsor has to comply with the new requirements or wants to be ready for what may come, familiarity with the GDPR and how it relates to sweepstakes and contests is critical.

In a (very tight) nutshell, the GDPR protects data subjects (EU residents) when providing personal data (anything provided online that can identify the person) from a company's collection or use of personal data without the data subject's consent. Consent is the *sine qua non* of the new regulation and *tres* specific: any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which she provides a statement

or clear affirmative action signifying agreement to the processing of her personal data. GDPR Art. 4 Sec. 11.

This means that if a U.S. company is running a sweepstakes open to EU residents, it is subject to the GDPR and has specific obligations to obtain consent for the collection and use of the entrant's personal data, to provide notice of the entrant's rights, and to comply with the entrant's directives for use of her personal data.

Complying With the GDPR for Sweepstakes and Contests

The GDPR does not contain any specific terms covering sweepstakes. Nevertheless, a sponsor should be aware of three areas: notice of rights, consent, and data handling.

Notice Requirements

The sponsor must have a GDPR-compliant privacy policy, clearly available to the entrant and in easy-to-understand language. The topics to be covered include: the information collected; how and why it's collected; how it's used; and how it's secured.

While these disclosures are already common in the U.S., additional GDPR-specific information should also be included: the controller's contact information; the use of automated decisions; the legal basis for processing data; and the user's eight rights.

The Data Subject's Eight Rights

The GDPR requires that sponsors provide clear and easily understood notice of the data subject's eight rights before any personal data can be collected. GDPR Arts. 12-23. For sweepstakes, these rights should be in the privacy policy, which is clearly disclosed (or linkable) prior to entry, and preferably in a succinct notice on the entry page itself.

1. **Right to be informed.** The sponsor must inform the entrant of her rights under the GDPR.

2. **Right to access.** The entrant can obtain information on whether, why, and how her personal data is being processed.

3. **Right to rectification.** The entrant can have the sponsor correct inaccurate personal data.

4. **Right to erasure.** The entrant can have the sponsor erase her personal data.

5. **Restriction of processing.** The entrant can request that the sponsor restrict processing when her personal data is inaccurate, when processing would be unlawful, or when the data is no longer needed.

6. **Data portability.** The entrant can obtain her personal data to transmit to another controller.

7. **Right to object.** The entrant can object at any time to the processing of her personal data, including when it is used for direct marketing.

8. **No automated decision making.** The entrant can object to profiling — the automated processing of her personal data to evaluate certain personal aspects such as her economic situation, personal preferences, and interests.

The theme is that the entrant is in charge of her personal data, even after it's given to the sponsor.

Although the GDPR does not offer specific guidance for necessary disclosures in the official rules, the following paragraph may be sufficient for GDPR purposes:

> **Privacy Notice for EU Residents:** The General Data Protection Regulation (GDPR) provides a number of protections for the collection and use of your personal data. Any personal data collected from you shall be subject to the sponsor's privacy policy located at www.XXXXXXXX and the GDPR. The sponsor will only use your personal data for the purposes of administrating this contest, unless you provide consent signifying your agreement to any other processing or use of your personal data. You can withdraw your consent at any time by [insert method].

Consent

When collecting any personal data online for sweepstakes:

1. The sponsor can only collect what is necessary to administer the sweepstakes, perhaps name, address or email, without obtaining specific consent.

2. The sponsor must provide a specific option to opt in to each use of personal data other than for administration of the sweepstakes. (The sponsor cannot use a negative option or require a person to opt out.) Each option must be stated separately, in easy-to-understand language.

3. The sponsor must inform the entrant that she can withdraw consent at any time, for any or all consents given, and provide an easy method to do so.

4. Without consent, the sponsor can only use the personal data for the limited purpose for which it was given and must delete the personal data after its purpose is completed.

5. If an entrant is under 16 years of age, the sponsor must make reasonable efforts to obtain consent from the parent or legal guardian. GDPR Art. 8.

As a practical matter, the online entry form should have specific/separate opt-in options, links to the official rules and privacy policy, and notice and method to opt-out—all provided prior to entry.

Security of Personal Data

The sponsor must have appropriate measures to ensure security of personal data, including encryption, resilient processing systems, tested safety methods, breach notification, and recordkeeping, if appropriate. GDPR Arts. 24-43. The sponsor must also report personal data breaches within 72 hours. GDPR Art. 33.

Penalties

In addition to judicial claims for damages, the GDPR provides for monetary penalties (in the U.K.) of up to 10 million pounds ($13.9 million) for data security breaches, and up to 20 million pounds for infringement of an individual's privacy rights, based upon the nature, gravity, and duration of the offense, whether it was intentional or negligent, and whether the damage was mitigated.

A sponsor may not have much time to tackle the GDPR's steep learning curve. But when in doubt, a

sponsor should adhere to the GDPR's principles: transparency, consent, and accountability. Or, with a nod to upcoming Mothers' Day: If Mom would think it's a bad idea, it probably is.