EDM paperfreedm

GDPR's impact on data capture

By Andrew Shaw, Group CCO

Although some content suggests it, The General Data Protection Regulation (GDPR) is not designed to disrupt your current data capture strategy. That said, the new law does have some important implications for the ways in which businesses collect and manage the personal information of EU residents.

This piece gives an overview of how the GDPR changes the environment surrounding data capture and offers tips on maintaining a compliant data capture strategy.

GDPR: The need to view data capture in a new light

From policy applications, customer surveys and mailing list sign-ups, through to behavioural data taken from your website, personal data in multiple online and offline formats is captured by businesses in an ever-growing range of ways.

This can give rise to organisations taking an unlawful approach to personal data under their control, which is the type of attitude to data capture that GDPR seeks to diminish. Instead, it demands that you take into account the following:

Data capture should be controlled
Rather than attempting to catch as much as you can, any personal data captured should be limited for what is necessary to meet defined purposes. Those purposes need to have a lawful basis, clearly explained to the individual, and once the defined need for it has ended, the data processing should also cease.

Post-capture, subjects retain considerable rights over their personal data
GDPR enhances existing rights – for instance, by stipulating that most Subject Access Requests (SARs) must be responded to free of charge. Through the new rights to erasure and data portability, it also extends the level of control individuals have over their data.

An ongoing obligation to "protect the data rights and freedoms of individuals"
Art 25 obliges organisations to adopt the principles of Privacy by Design and Privacy by Default. When a new method of data capture is considered and implemented, you must ensure that "appropriate" safeguards to protect the rights of individuals are effectively hardwired into it. You must also ensure that only the data required for specific processing activities is actually processed.

> "The General Data Protection Regulation (GDPR) is not designed to disrupt your current data capture strategy"
>
> **- Andrew Shaw, Group CCO**

Building data minimisation into data capture

A customer survey provides a useful illustration of this. You explain to your customer that the purposes of this survey are to gauge the quality and effectiveness of a particular offering – and to inform future product-specific improvements. The data you capture should be limited to achieving this, taking care not to stray into the territory of building up a 'potted profile' of that customer for wider marketing purposes.

Is the personal data you are seeking to acquire "adequate, relevant and limited to what is necessary" for its intended purpose? The fundamental GDPR principle of purpose minimisation, (Art. 5 1. (c)) requires you to establish this in all instances of data processing – including capture.

Establishing a lawful basis for instances of data capture

To avoid the inference of data mining, organisations must assess and be able to demonstrate the legality of each data capture activity, with reference to one of GDPR's six bases for lawful processing.

Examples of appropriate categorisation include the following:

- **Consent:** Where data is captured in order to dispatch marketing material to the data subject.
- **Contractual obligations:** The collection of address information and the subsequent transmission of this to a courier to enable product delivery.
- **Legal compliance:** Where key data is obtained at the outset of the relationship in order to meet your anti-fraud, know-your-client obligations.
- **To protect the vital interests of the data subject:** Obtaining health and next-of-kin information for health & safety purposes.
- **Public interest/official authority:** The capture of sensitive demographic information for the purposes of government-led diversity impact assessments.
- **Legitimate interest:** Data capture for the purposes of tailoring personalised offerings for the data subject, where this is a key component of your business model and where the method and aims of data capture do not materially impact the rights and freedoms of data subjects.

Consent

In all instances where you rely on the lawful basis of consent for capture and processing, you must ensure that GDPR's requirements for obtaining that consent are met (set out in Art. 7). This includes the following:

The ability to demonstrate that consent has been given: In practical terms (in the case of marketing, for instance), this is likely to require a database distinguishing between those customers who have positively opted into communications, along with a suppressions list of those who have not provided consent – or who have subsequently opted out.

Unpacked, clear consents: GDPR prohibits a 'bundled' approach to consent – i.e. where customers are invited to give consent to various unconnected data-related activities at a single stroke. Both on the Web and for offline data capture forms, you need to ensure that positive, opt-in consents for specific activities are distinguishable from other matters. These should be set out in clear, easily understandable language.

Capable of being revoked: Consent should be capable of being removed by the data subject at any time. You need to have mechanisms in place for this (e.g. unsubscribe buttons on each e-newsletter).

Enabling the right to data erasure

The new "right to be forgotten" is a major change, allowing data subjects to request erasure of data, provided that certain conditions are met. This has the following implications for your data capture strategy:

- **Data capture must be accompanied by appropriate data management:** To enable erasure requests (and general SARs) to be actioned, you need the ability to track precisely what personal data your organisation holds on individuals, its purpose, where it resides and in what format. Without this ability, it will be difficult to respond "without undue delay", as is required under the Act.
- **Appropriate classification is vital:** GDPR does not usher in "total erasure on demand" – and there may be circumstances where ongoing retention of captured data is necessary. As it comes into your control, you need the ability to ensure that appropriate retention rules are applied to each captured data set.

Summary - How to ensure your data capture is GDPR compliant

Establish a lawful basis for each instance of data capture. Here, be especially wary of over-reliance on the ground of 'consent' – bearing in mind that this can be easily revoked.

Ensure a transparent approach to communications. As well as ensuring clear consents, this also includes possible updates to your privacy policy to ensure that the purpose, methods and timeframes for processing, as well as the data subjects rights, are all explained clearly.

Adopt appropriate safeguards to help stay on top of your obligations. A Digital Mailroom can be especially valuable on this front. With it, all personal data entering your organisation, whether electronic or in physical form, enter the same process flow. It is automatically transferred to the right location (e.g. a customer case file), enabling you to see precisely what you hold at any particular time. Retention categorisations can be applied automatically, enabling you to respond to erasure and subject access requests swiftly and appropriately. A Digital Mailroom gives you complete control over the data capturing process, ensuring that you keep your client's data secure, and ultimately keeping the entire process GDPR compliant.

For more information on how EDM Group's Digital Mailroom technology can help ensure compliance while encouraging more efficient data capture strategies, take a look at our Digital Mailroom hub.

Author

Andrew Shaw

Group CCO

Email: Andrew.shaw@edmgroup.com

LinkedIn: https://www.linkedin.com/in/andrew-shaw-8472291/

Visit: www.edmgroup.com