Katten

Katten Muchin Rosenman UK LLP

Privacy Matters

General Data Protection Regulations (GDPR)–How to Achieve Compliance

GDPR 25 May 2018

In our last issue, we considered the questions of *what*, *when*, *where* and *how*. This week, we cover the key question of *why*. Before requesting personal data from your customers, your suppliers and your employees, you must always consider why you need it. "Just because" is unlikely to cut it!

Checklist – Processing Personal Data Legally

Don't Fall at the First Hurdle

Ensure you're covered with a legal basis to process personal data:

- Do you have specific, affirmative and informed consent from the individual?

> **Top Tip:** *Because individuals can withdraw consent, it is often more predictable for businesses to rely on a legal basis other than consent when collecting and processing personal data.*

- Is the personal data necessary to comply with a contract to which the individual is a party?
- Is it necessary to process personal data to comply with the law?
- Is it necessary to process personal data to protect the health and well-being or vital interests of the individual?
- Is it necessary to obtain personal data from individuals in order for a business to run (*e.g.,* processing the names of your employees to employ them)?

> **Top Tip:** *Collecting and processing sensitive personal data (e.g., political opinions, health data, racial or ethnic origin) or personal data from children (ranging from 13 to 16, depending on the member state) requires additional consideration. Know your demographics, the types of data elements and seek advice for any unique requirements or applicable local laws.*

Collected Legitimately

- Inform the individual why you need their personal information.
- If these reasons change, you must inform the individual.

> **Top Tip:** *Keep individuals informed by regularly reviewing and updating your privacy policies and/or customer notices. Conduct reviews when there is a significant change to your collection or processing activities. Bi-annual reviews work well.*

Less is More

- Only collect what you need and keep the processing of personal data to a minimum.
- It is illegal to process more data than is necessary. Data minimization is not only important for compliance but can also reduce unnecessary liability.

> **Top Tip:** *If you need only names and email addresses for a mailing list, consider why you would need to collect an individual's date of birth or other information.*

Keep Only for as Long as Necessary

- Keep personal data you store about an individual:
  - secure;
  - up to date; and
  - relevant and accurate.
- Out-of-date personal data, or data that does not serve the purpose for which it was originally collected, should not be kept.
- Erase stale or irrelevant data.
- *Caveat:* You can keep it as long as it is for:
  - archiving purposes in the public interest; or
  - scientific, historical or statistical purposes.

> **Top Tip:** *Review your data retention policies and technical systems regularly to ensure that you are complying with data minimization practices and requirements.*

Attention to Detail – Record of Processing

- Implement and maintain a Record of Processing. The record should include, at a minimum, identification of the controller(s) and processor(s), the purpose for processing the personal data and a description of the categories of data.
- Third-party vendor contracts that assist you with personal data processing must use compliant language. Review your vendor agreements and update them as necessary.

> **Top Tip:** *As the data controller (i.e., the entity or person that determines the purposes and means of the data processing), you are responsible for the third-party vendors that assist you with data processing activities. Familiarize yourself with your vendors' processing activities and security practices to ensure they are compliant and meet your standards.*

Security

Keep the personal information secure and protect it against:

- unauthorised or unlawful processing;
- accidental loss;
- destruction; or
- damage.

> **Top Tip:** *Have security systems in place like password protection and security policies designed to ensure that the data can only be accessed by people who actually NEED to access it. If possible, pseudonymise the information to add an extra layer of security. Regularly review and update your security systems to ensure that they are current and comply with the requirements of the GDPR.*

Stay tuned for our next infographic setting out an example of a data flow map.

If you have questions about the GDPR or about the topics covered in *Privacy Matters*, please contact any of the following Katten attorneys:

Christopher Hitchins
+44 (0) 20 7776 7663
christopher.hitchins@kattenlaw.co.uk

Doron S. Goldstein
+1.212.940.8840
doron.goldstein@kattenlaw.com

Alan D. Meneghetti
+44 (0) 20 7770 5232
alan.meneghetti@kattenlaw.co.uk

Matthew R. Baker
+1.415.293.5816
matthew.baker@kattenlaw.com

Sarah Simpson
+44 (0) 20 7770 5238
sarah.simpson@kattenlaw.co.uk

Joshua A. Druckerman
+1.212.940.6307
joshua.druckerman@kattenlaw.com

Brigitte Weaver
+44 (0) 20 7770 5235
brigitte.weaver@kattenlaw.co.uk