The First Step in Developing a GDPR Compliance Strategy

Assess Your EU Personal Data Flows

By:Faith D. Kasparian
May 08, 2018

The first step in developing a GDPR compliance strategy is to assess the ways in which your business intersects with EU personal data. To facilitate this assessment, we have prepared the following EU Personal Data Flows Questionnaire. The responses to these questions will not only help your business understand its EU personal data flows but will help us develop a compliance strategy that is tailored to your business. We invite you to contact us if we can support your GDPR compliance needs.

1. What types of personal data (any information about an identified or identifiable natural person) about EU data subjects (individuals residing in the EU) does your business collect, handle, store, or access?

(a) If different types of personal data are collected/handled based on the category of individual (i.e., employee, website visitor, customer, business partner, etc.), specify this information by category of individual.

(b) Consider whether your business has access to personal data in connection with providing support services.

(c) Specify whether any of this data is "sensitive" – that is, data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life/orientation.

(d) Specify whether you process any children's personal data.

2. From whom do you collect or receive personal data about EU data subjects – direct from the individuals concerned or from a third party?

3. How is each category of personal data about EU data subjects used in your business and for what purposes?

4. For each category of personal data:

(a) is your business the entity that is the "owner" of the data – the entity that has the right to determine the purpose and means for which the data is handled; or

(b) is your business simply handling the data on behalf of the entity that is the "owner" of the data?

5. For each category of personal data about EU data subjects, under what circumstances do you share that personal data with third parties?

(a) Specify the names of all third parties with whom you share or otherwise provide access to personal data about EU data subjects and the purpose of such sharing or access (this could include anyone who hosts your website/trading platform or with whom you have arranged for data back-up or disaster recovery).

(b) In particular, specify whether: (i) the third party is simply handling the data on your behalf and at your direction (as an example, in order to provide a service to you); or (ii) the third party will have independent rights, such as license rights or ownership of the personal data that is shared.

(c) Please provide copies of any "template" agreements with such third parties (or let us know the number and type of such template agreements you have).

(d) Please provide a copy of any existing executed agreements with third parties with whom you share or provide access to the personal data (or let us know the number and type of executed agreements you have executed).

6. For each category of personal data about EU data subjects, do you transfer the data outside the EU and if so, to where and for what purposes do you transfer it?

7. Please provide any existing privacy notice or privacy policy that addresses information about human beings (including personal data from EU data subjects).

8. Please provide a copy of any existing agreements with any EU data subjects – including any online terms or consent agreement with any EU data subjects. This could include details of the information that you give to EU data subjects when collecting or after having been given their personal data.

9. Please provide copies of:

(a) your existing data security policy; and

(b) any data breach response/notification policy that apply to information about human beings (including personal data from EU data subjects).

10. Please provide any existing policies that address how your business handles requests from individuals exercising rights with respect to their personal data.

11. Do you have any existing policy for data retention and disposal? If so, please provide a copy.

12. Do you have a person within your organization who is primarily responsible for data protection reviews? If so, please provide his or her contact details.

For more information, please contact **Faith Kasparian**.