IAB CANADA GDPR UPDATE

13 KEY COMPLIANCE STEPS
FOR CANADIAN DIGITAL MEDIA AND ADVERTISING COMPANIES
FEBRUARY 2018

The Reach of the EU GDPR in Canada

On May 25, 2018, the General Data Protection Regulation (GDPR) will impact companies in Europe and around the world. The penalties for violating are potentially severe – Fines of €20 million or 4% of your annual worldwide revenue (whichever is higher).

Your digital media or advertising businesses in Canada will be directly impacted by the GDPR if your company processes personal data of EU residents where the processing relates to:

- offering goods or services to individuals in the EU; or
- monitoring the behaviour of individuals in the EU on the internet, which may include tracking for behavioural advertising purposes.

The GDPR sets out a holistic set of rules governing the collection, creation, use, disclosure, storage and other processing of "personal data", a concept defined broadly as "information about an identified or identifiable natural person".

GDPR's rules are prescriptive, and need to be operationalized across your company's systems and processes. Considerable time and organizational effort is required to comply with this statute.

The following is a checklist of 13 key steps for your company GDPR compliance efforts:

1. Ensure senior management of your company is fully aware of the requirements under the GDPR and the possible impact of non-compliance, and that senior management dedicates sufficient resources to your company's ongoing compliance initiative.

2. Appoint a Chief Privacy Officer, and form a privacy committee of key stakeholders in your company whose business units are involved in the processing of personal data.

3. Develop internal policies and implement technical and organizational measures to incorporate "privacy by design" into your company's systems.

4. Prepare a data inventory and map of your company's data processing activities so you understand where personal data is sourced, how it is collected and used, where it is transferred and disclosed, where it is stored, etc.

5. As part of your data inventory, carefully review and map your company's international personal data flows, in particular the flows of data from the EU, and consider what existing data transfer mechanisms are in place to ensure your company complies with the GDPR's transborder data flow restrictions.

6. Conduct "privacy impact assessments" for high-risk areas of personal data processing.

7. Ensure that, in relation to each type or category of processing, your company has identified and documented the grounds for lawful processing (e.g. consent or, where the legitimate interests ground is being used, what the legitimate interests are).

8. Develop a process for recording consents, including a record of what each individual data subject consented to.

9. Review and update consumer facing notices/privacy statements.

10. Review and enhance internal company policies to ensure compliance with all GDPR requirements, including policies and procedures addressing data subject rights, which include "data portability", rights of access, rights of correction, and rights of erasure ("right to be forgotten").

11. Review and enhance your company's data breach response and notification procedures to meet the 72 hour deadline in respect of notification to the data protection authorities.

12. Implement a company-wide training program covering data/privacy protection.

13. And, most critically, ask questions! Many provisions of the GDPR are highly technical and can be complicated to comply with. If you have any questions about the GDPR (or other privacy laws) or your company's data protection compliance efforts, ask your company's Chief Privacy Officer or in-house counsel.

* * *