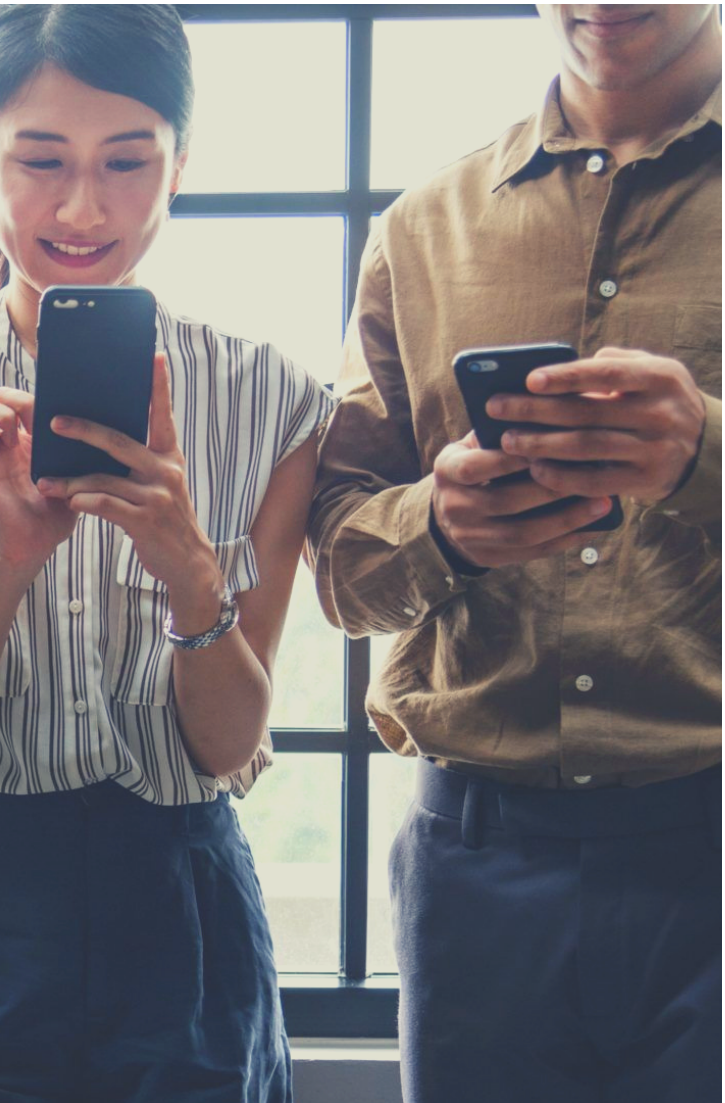
“WHAT ARE THE GDPR REGULATIONS FOR PERSONAL DATA IN ELECTRONIC RECORDS SUCH AS SOCIAL MEDIA, VIDEO, AND INSTANT MESSAGES?”

ARMA Q&A

GDPR REGULATIONS AND ELECTRONIC RECORDS



Since May 28, 2018, the General Data Protection Regulation (EU) (2016/679) (GDPR) has been in force. The GDPR is not new; it is an updated replacement for the now repealed Data Protection Directive (1995/46/EC).

Article 3 of the GDPR states that it applies to the processing of personal data by a controller or a processor, whether inside or outside the European Union (EU). A controller is an organization or individual who processes personal data. For example, a controller could be a retailer with an online store that stores its customers’ information. A processor is an organization or individual who processes personal data on behalf of the controller. A processor could also be a cloud service provider storing personal data for clients. Organizations located outside of the EU doing business in EU states could be subject to the GDPR if those organizations process personal data from an EU state.

The GDPR increases fines for noncompliance to a maximum 20 million EUR or 4% of the total annual worldwide turnover, whichever is higher.

Also, the GDPR is subject to whatever data protection legislation is passed by specific EU states.

Some find the GDPR to be long and complex and it is. But, at its heart, the GDPR operates on a basic principle: an organization can only work with the personal data of an individual if it is permitted by law or with the consent of that individual.

Article 5 of the GDPR requires that personal data be processed lawfully, fairly, and in a transparent manner. Further, Article 5 requires that personal data shall only be collected for specified, explicit, and legitimate purposes and not further processed in a way that is incompatible with those purposes.

Electronic records are not defined in the GDPR. However, electronic records, such as social media, video, and instant messages, come under the GDPR umbrella since they could be "personal data." Personal data is given a wide definition in Article 4. It means "any information relating to an identified or identifiable natural person." The focus in the GDPR is neither on the format of the record nor on the specific technology producing the record. Instead the focus is whether the record identifies a natural person. Examples of information in an electronic record that identify a natural person include a person's name, cell phone number, ID number, email address, and location data or online identifier, like an IP address or cookie.

What is new in the GDPR is that Article 5 applies the principle of accountability, in that the controller of personal data must ensure compliance with the GDPR and prove that compliance.

Whether they are controllers or processors of personal data, organizations can prove their compliance with the GDPR by maintaining records of their processing activities. Organizations can designate a data protection officer to ensure GDPR compliance. Organizations can conduct data protection impact assessments to identify and implement measures to mitigate risks to personal data protection.

about the author

Stuart Rennie

For the past 18 years, Stuart has been the Legislation and Law Reform Officer at the Canadian Bar Association, British Columbia Branch (CBABC). He provides consulting advice on proposed BC legislation, advises lawyers on BC statutes and regulations and provides policy and information governance advice.