Articles + Publications | June 1, 2023

Lessons From the GDPR on the Sunset of the CCPA's Personnel and B2B ?Exemptions

Privacy & Cybersecurity Newsletter

WRITTEN BY

Theodore P. Augustinos | Nick Elwell-Sutton

RELATED OFFICES

Hartford | London

As of January 1, 2023, the personal information of personnel (including job applicants, employees, officers, directors and contractors), and of business to business contacts, is subject to the California Consumer Privacy Act ("CCPA"). This is because of the January 1 sunset of the prior exemption for personnel and B2B data.

Given that the GDPR never had exemptions for personnel and B2B data, what lessons can practitioners in the U.S. learn from the experience of our friends and colleagues in the EU? While it is not yet known whether the CCPA will take the same approaches observed under the GDPR, it is likely that CCPA enforcement and consumer activity will be informed by the GDPR's experience.

In the EU, data subjects ("consumers" under the CCPA) who are personnel or B2B contacts now frequently submit data subject access requests ("DSARs"). Requests to know, delete and correct, and to exercise other rights from these individuals have only been permitted under the CCPA since January 1, 2023. How have these requests been handled in the EU? What should U.S. businesses subject to the CCPA do to comply, given the sunset of the important personnel and B2B exemptions?

- Data controllers will need to respond to information requests – they can and do happen and there is only one direction of travel. Privacy notices provided to data subjects must disclose consumers' rights, including the right to make a DSAR and to complain to the regulator if dissatisfied with the response. This means that consumers' rights, which may otherwise be obscure, are to be brought specifically to the consumers' attention.
- The request to know has become the weapon of choice for what effectively amounts to pre-litigation discovery. It is a quick, no cost and easy way to obtain information that a consumer would not otherwise be able to obtain outside the formal litigation process, and is frequently used by employees to gain access to emails and messaging exchanges, reports, assessments and reviews concerning them by others within an organisation and which has the ability to provide insight as to whether the consumer may have a cause of action. A common example would be an email exchange between supervisors about an employee's performance. In any workplace dispute, the first shot fired is now inevitably a DSAR from the employee.
- Because of this, there is a need to start educating personnel to practice defensive internal communications. At best, there is the risk of corporate or professional embarrassment through inappropriate comments in emails and at worst the risk of "smoking gun" documents giving rise to discrimination, harassment or defamation in addition to remedies for unlawful processing under GDPR. This has given rise to a common phraseology: "dance like nobody is watching; email like you're reading it back in court."
- Businesses must respond to DSARs promptly, and so it is important to have in place an action plan to recognize requests, and procedures on how to respond.

- From experience in the EU, if a request is made, the following steps provide a framework for responding to consumer requests under the CCPA:
  - Designate a single point of contact for both internal response actions and for the consumer.
  - Acknowledge response promptly, and keep the consumer updated.
  - Try to agree with the consumer as to the scope and any exclusions. For example, is the consumer prepared to agree that any emails they sent, received or were copied to can be excluded from the scope? In many cases what the consumer is really after is information about them they do not have and agreeing to exclude what they have already seen can reduce significantly the scope of for the search for personal data. Similarly, it can sometimes be possible to agree to limit the scope of the request by topic, time period, or custodians.
  - It may also be possible to agree to keywords with the data subject. If the issue is, for example, about a reduction in force (RIF) process, agreeing to likely keywords (such as “RIF”, “termination”, “redundancy”) may limit the scope of the search.
  - Most businesses hold data in a number of places and across applications. It is therefore important to understand where data may be held and to carry out a mapping process to identify all likely sources – email, internal messaging apps (Slack, Teams), document management systems, other applications, and hard copy files.
  - If your internal systems do not have the ready functionality to carry out searches then making systems changes to allow that will be a priority so they can be properly searched and data identified, harvested, and exported.
  - Many businesses also have less formal methods of communication, such as text messages and WhatsApp, and which can give rise to difficult legal issues about whether data on those devices falls within the scope of the data for which the business is responsible. While the position in the U.K. around this is not wholly settled, the preponderance of views is that if the business permits communications on either devices it provides or employees’ personal devices, it will have responsibility for that data.
  - Given the tendency for email chains, consider using an application that will de-thread and de-duplicate them so that there is only a single copy of the data set – which will help reduce the overall number of documents.
  - Once a single data set has been complied, it must be reviewed to identify relevance as being personal data, whether any exemptions apply and whether irrelevant information (for example data about others or confidential matters) need to be redacted. At this stage, despite the recent advances in AI and litigation support platforms, they are not yet advanced or sophisticated enough to undertake this. Even a modest DSAR may generate several thousand responsive document hits each of which will need a manual review.
  - From experience, about 38 documents an hour can be reviewed so for even 1,500 responsive documents that’s around 39 hours of review time, which illustrates the “hard yards” involved in complying.
  - In the U.K., there are a number of exemptions available. These include legal privilege, management forecasting, negotiations and confidential references. The CCPA also has exemptions, including for compliance with legal process and maintaining privilege.
  - Any business can adopt one of two approaches to third party data contained within a document and other information not relevant to the request (e.g. confidential information). Irrelevant data can be redacted, or alternatively, only the relevant data extracted from the documents and then populated into an otherwise blank document and the consumer is then provided with either the redacted data set or only the relevant extracted data.
  - There needs to be a secure method of transmission to the data subject, typically by providing a secure weblink for the data subject to review, or by sending them encrypted files. In addition when responding a business should explain what it did and how it went about it so as to be able to demonstrate compliance.
  - There should also be an audit trail in case a complaint is made to the regulator, again to be able to demonstrate compliance.

- From the U.K. experience since the advent of GDPR in 2018, the additional observations may be instructive:
  - Regulators are generally very favorable toward consumers and their ability to exercise their rights, but they are swamped with complaints so regulatory action and intervention takes a long time. In most cases the approach is remedial rather than penal.
  - Although the issue of proportionality features in the approach to complying with a consumer request, a recent U.K. case held that in excess of 100,000 documents did not mean compliance was disproportionate. Therefore, the use of cost or the technical burden of compliance should be weighed carefully, and

conservatively, before denying a consumer request on this basis.
- Regulators are reluctant to accept allegations of abusive requests as a reason for non-compliance and it has been held that the purpose of the DSAR is blind. Therefore, bad faith, ulterior purpose or the purpose of annoying the business are not valid reasons for non-compliance. The regulator is even reluctant to accept blackmail as a reason not to comply. Being prescriptive as to how a request is made or placing obstacles in the way of exercising data rights is frowned upon, and even requests made via social media channels (e.g. a business's Twitter feed) have been held to be validly made.
- Consider reviewing data retention periods and their appropriateness. The less data you hold, the less there is to review and, if necessary, to hand over.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber