How not to write your GDPR-'compliant' data protection policy

May 22, 2018 Save This

Thomas Shaw, CIPP/E, CIPP/US

Editor's Note:

Thomas Shaw is the author of DPO Handbook — Data Protection Officers Under the GDPR. (https://iapp.org/store/books/a191a0000027yHMAAY/)

The mark of an organization's commitment to data protection is shown through its data protection policy/statement/notice. A robust DP policy is essential. One of the things that a data protection officer is required to monitor is compliance with the DP policy. Unfortunately, some organizations are issuing what can only be termed "Caspar Milquetoast" DP policies. Caspar Milquetoast was a cartoon character who was timid, bland and inoffensive. Obfuscating their data collection and processing activities on the personal data while using the keywords from the GDPR, some controllers are publishing revised DP policies that under-inform or misinform their customers.

The Article 29 Working Party's recent transparency guidance provides very helpful direction. It states,

empowers data subjects to hold data controllers and processors accountable and to exercise control over their personal data … the quality, accessibility and comprehensibility of the information is as important as the actual content of the transparency information, which must be provided to data subjects … The information should be concrete and definitive; it should not be phrased in abstract or ambivalent terms or leave room for different interpretations. In particular the purposes of, and legal basis for, processing the personal data should be clear … WP29 recommends as a transparency best practice 'that at the point of collection of the personal data in an online context a link to the privacy statement/ notice is provided.'"

It further states, "A central consideration of the principle of transparency outlined in these provisions is that the data subject should be able to determine in advance what the scope and consequences of the processing entails … the WP29 position is that controllers should not only provide the prescribed information under Articles 13 and 14, but also separately spell out in unambiguous language what the most important *consequences* of the processing will

be … Such a description of the consequences of the processing should not simply rely on innocuous and predictable 'best case' examples of data processing, but should provide an overview of the types of processing that could have the highest impact on the fundamental rights and freedoms of data subjects."

In the DPO Handbook (https://iapp.org/store/books/a191a0000027yGxAAI/), the basic components of an effective DP policy are described in chapter two. Knowing that the most significant source of transparency to almost all data subjects will be the DP policy, this document should bristle with useful information for data subjects. To illustrate the point of what EU data subjects can face when GDPR begins, a real DP policy is analyzed to try and understand a better way to write these documents to provide the most information to data subjects. DPOs responsible for assessing and advising on GDPR compliance should be on the forefront of getting controllers and processors to write DP policies that provide the maximum, not the bare minimum, amount of valuable information to data subjects.

The provisions

Eight provisions of a real DP policy recently revised for the GDPR are analyzed below, with the controller's identity anonymized. Fully answering the queries after each quoted provision would make these provisions better by more fully informing the relevant data subjects. DPOs should remember the transparency exhortations of the WP29 when revising their DP policies, but always do so in a legally defensible manner.

"We collect personal information from you, for example when you … We also collect information through our website, apps, social media, discussion forums, market research and our CCTV footage."

What is meant by "personal information," a similar but purposely different wording than the term "personal data" defined in the GDPR? What types of personal data is collected directly from the data subject? What type of information (is it personal data?) is collected indirectly via websites, apps, social media, for what purpose is it collected, who is collecting it, who is it disclosed to, and under what legal basis is it collected? The minimum Articles 13–14 requirements are the purposes of processing, legal basis, recipients, overseas transfers, retention periods, obligations to provide personal data, and the consequences for not doing so, automated decision-making, legitimate interests if any, source of data if not the data subject, and any further processing plus data subject rights. Per GDPR Recital 39, data subjects should generally be "made aware of the risks, rules, safeguards and rights in relation to the processing of personal data." This would include any processing where collection of personal data is not obvious. The WP29 includes the providing data subjects the compatibility analysis for any further processing.

"We may collect information to identify you through voice, facial or fingerprint (biometric data) recognition technology. We always ask for your consent to do this."

Biometric data is a special (sensitive) category of data whose processing requires the explicit consent of the data subject, extra care as to the security of the data including DPIAs (biometric data used cannot be changed like a password if it is disclosed), and minimal retention periods. The explicit consent requires providing the data subject with certain information and getting a definitive response. These additional requirements are not explained sufficiently nor are consequences of the high-risk processing of biometric data.

"Our websites use 'cookie' technology. A cookie is a little piece of text that our server places on your device when you visit any of our websites or apps. They help us make the sites work better for you."

A cookie comprises data that can be used to track the preferences and activity of a user, and there are clear privacy differences between first- and third-party cookies and between session and permanent. These distinctions are important to describe. Consent is required before a cookie is placed on a device (per the ePrivacy Directive). How is the consent obtained and how is it different than consent to process personal data? How does the use of cookies make "the sites work better for you"? This is a common platitude in DP policies, but what are consequences of the use of cookies (e.g., for behavioral tracking of users' internet activity?) If users are being monitored through the use of cookies or similar technology, this must be disclosed.

"How we keep your information safe. We protect your information with security measures under the laws that apply and we meet international standards. We keep our computers, files and buildings secure."

This wording actually says almost nothing. What types of information security measures are used, for example? Does the controller employ end-to-end encryption and ensure that they control the encryption keys? What specifically are the international standards? Are they security-related standards (e.g., ISO 27001)? And why has the controller not become certified by an independent assessor instead of apparently self-certifying ("we meet international standards")? The key controls used to keep computers, files, and buildings secure should be stated, as then the controller can be held liable if those safeguards are not deployed effectively, demonstrating true confidence in their information security regime.

"How long we keep your information. To meet our legal and regulatory obligations, we hold your information while you are a customer and for a period of time after that. We do not hold it for longer than necessary."

Who defines necessary? (https://iapp.org/news/a/excessive-personal-data-who-decides/) The durations that major categories of data are retained should be clearly stated, as well as the most common legal and regulatory basis for retaining the information that long, the effect this has upon the right to erasure (to be forgotten), and the secure disposal or anonymization techniques employed when the data is no longer needed.

"To use your information lawfully, we rely on one or more of the following legal bases: performance of a contract; legal obligation; protecting the vital interests of you or others; public interest; our legitimate interests; and your consent."

Reiterating every possible legal basis from Article 6 tells the data subject nothing about their particular processing. The data subject must know, for major categories of processing, which legal basis is used. If based on consent, then describe the information that will be provided and when, and discuss consent withdrawal. If based on a legal obligation, name the statute. If a contract, how the contract is formed. If it is based on a vital interest of the data subject, list the possible vital interests. If it is the controller's legitimate interest, list possible interests and how it will be balanced against the rights and interests of the data subject. As all of these except consent allow for the collection of only necessary data, describe how necessity is determined. Specific differences from these general descriptions in the DP policy should be disclosed at collection.

"We sometimes use technology to help us make decisions automatically."

A data subject has the right to not be subject to decisions based solely on automated processing, under Article 22, if such processing produces legal effects or significantly affects them. The exceptions are for performance of a contract between the parties, with explicit consent, or based upon a law but in all cases, safeguards must exist for the data subject's rights, freedoms, and interests. This is not explained, nor is an ability to have human intervention in the decision-making process or to understand the algorithm used. "You may have the right to … object to us … using automated decision making." How are data subjects informed that automated decision making has taken place, how do they object, and is it 100 percent certain that the phrases "making decisions automatically" and "automated decision making" are the same thing?

"***We may transfer your personal information outside of the European Economic Area (EEA) to help us provide your products and services. We expect the same standard of data protection is applied outside of the EEA to these transfers and the use of the information, to ensure your rights are protected."***

The transfer of personal data outside the EEA should be the exception instead of the rule (https://iapp.org/news/a/a-deep-dive-into-the-schrems-ii-case/) and some justification for it should be stated, as just about any processing possible can be performed within the EEA. When necessary, the transfer mechanism relied upon should be clearly stated in the policy, as well as any impacts on the legal rights of data subjects in case of a violation of their data protection rights in this third country. The controller is the party negotiating with these third parties and can ensure contractually that the third party will, at all times, have the same levels of protection,

and if they do not, will have appropriate penalties stated in the agreement to include immediate deletion of all personal data received and compensation to the affected data subjects. Finally, WP29 advises that “Language qualifiers such as 'may,' 'might,' 'some,' 'often,' and 'possible' should also be avoided."

photo credit: ThoroughlyReviewed Legal Contract - Must Link to https://thoroughlyreviewed.com (http://www.flickr.com/photos/143842337@N03/34247035975) via photopin (http://photopin.com) (license) (https://creativecommons.org/licenses/by/2.0/)

Author

Thomas Shaw, CIPP/E, CIPP/US

Share This

Tags

Privacy Law (/tag/privacy-law) Privacy Operations Management (/tag/privacy-operations-management)

Pease International Tradeport, 75 Rochester Ave, Suite 4
Portsmouth, NH 03801 USA • +1 603.427.9200