CampusGuard News

9/20/2018

GDPR: Updating Your Privacy Notice

By now most organizations have determined if and how the European General Data Protection Regulation (GDPR) applies to them, have begun tracking those individuals in the EU they interact with, and have begun updating their policies and processes accordingly. The organizational privacy notice is one of the documents that must also be updated to better align with this new regulation.

Your privacy notice is how you explain to users, at the point of data collection, what you are going to do with the information they provide. Every application you access has a privacy policy or user agreement that you must agree to before you can proceed. You always read every word of these notices before clicking AGREE, right? Or, are you in the large majority of users who just moves the scroll bar down, clicks AGREE, and moves on? We found a recent report that calculated the amount of time required for the average person to read every privacy policy for every website they had visited in the last year to be 244 hours. No wonder most people don't read them!

The GDPR is proactively trying to address this issue and states that, although full privacy policies will still be long, in-depth legal documents, under the regulation organizations have to provide users with an easy-to-read version. This notice, displayed at the point of consent or data collection, provides only the most relevant information and terms. This information must be:

- Concise, transparent, intelligible, and easily accessible
- Written in clear and plain language
- Made available to all free of charge

Within the GDPR, there are several requirements specifically addressing the organization's privacy policy and required consent for data collection. Each must include:

- a publicly accessible privacy policy that outlines all processes related to personal data,
- a clear explanation within the privacy policy outlining how collected data will be used,
- a process to inform existing users whenever your organization updates your privacy policy,
- a request for explicit consent before collecting or processing data from users, and
- a process for users to withdraw their consent as easily as it was initially given.

The good news is that you can still have an all-inclusive policy that addresses privacy requirements for GDPR and other standards (e.g. GLBA, FERPA). The policy will need to be updated to specifically inform users of their additional rights under GDPR. These include the right to be notified if data is transferred or processed for any purpose other than what it was collected for, their right to access the data, the right to erase/forget their data, and the right to withdraw their consent. The Data Protection Officer or primary point of contact that is responsible for questions or concerns related to data privacy should also be documented in the policy.

How you deliver this information can vary. Depending on where and how the information is being collected, the organization may utilize a variety of methods included dashboards, just-in-time notices, icons, and mobile device functionalities. Using these approaches, you can provide simple, easy to understand information initially, but also provide links for users to review the full policy as needed.

There are a number of great example privacy policies you can refer to (we've included a few below) but before you begin modifying these sample policies to fit your institution, there is prep work to be done. Begin by making sure you have a clear understanding of all personal data being collected and confirming what the organization does with it. Next, after a draft policy has been created, circulate the document to your staff to verify that the information is easily understood, clearly outlines what their data will be used for, and what their individual rights are. As with all other policy documents, regular reviews must be scheduled and updates made as needed. If plans are made to use the collected data for any new purposes, remember that the GDPR requires that the policy be updated and that you proactively inform those whose data is involved.

As you draft or update your current privacy policy, make sure it is addressing the questions below:

- What information is being collected?
  - Personal information, date of birth, ID numbers, nationality, employment history, educational records, family history, criminal records, etc.
- Who is collecting it?
  - Marketing, Admissions, Human Resources, Faculty, etc.
- How is it collected?
  - Website inquiries, application forms, email communications, etc.
- How will it be used?
  - Recruitment, admissions, donations, loan information, academic records, student support services, accommodations, parking, marketing, etc.
- How long will it be stored?
  - Data retention periods
  - Encryption or other methods for securing
- Who will it be shared with?
  - Employees, third-parties, loan companies, parents, etc.

Our team has reviewed several privacy policies that are publicly posted on the Internet and selected a few of our favorites below:

- https://www.lynn.edu/university-policies/statements/privacy-statement
- https://www.utah.edu/privacy/gdpr.php
- http://umich.edu/about/privacy/

If you have questions or would like CampusGuard to assist in reviewing or updating your institution's Privacy Policy, please contact your dedicated CampusGuard Team.

Some additional guidance from the Security Advisor team below:

> **[Ko]:** *Ah, September. Fall is in the air, college football is back in full swing, and we're finally past getting updates to privacy notices email notices from every third-party you've ever dealt with.* 😉
>
> *I have to admit, I have a love/hate relationship with the GDPR. As a consumer, I think this is the best thing to ever happen, and I plan on exercising my right to be forgotten and hopefully cut down on some targeted messaging. However, for data controllers using protected information, I feel that the pendulum has swung pretty far in the other direction and have put in some more difficult to implement restrictions.*
>
> *If we've learned anything at all in these past few months, it's not to behave like those companies that have made the unofficial "GDPR Hall of Shame." I get that we need to make consent easy to understand and granular, but, don't take a page out of the Tumblr playbook and make click 250 boxes to give or revoke consent.*
>
> *While we're at it, let's not forget to not set ourselves up to fail. The fastest way to become non-compliant with anything is to rapidly publish a new policy with no support or enforcement infrastructure. Make smart decisions that comply with the regulations that can also be implemented at 100 percent.*
>
> *As we talk about updating your privacy policies and privacy notices, it's important to note that these documents, especially the privacy notice, must be "transparent" and any consent received needs to be "unambiguous." Also, as a data controller you will also need to be sure that you are able to demonstrate that you have received the requisite consent from consumers.*
>
> *As the old adage goes, K.I.S.S.—Keep It Simple…er…for "Security's-sake!" Don't over-complicate your privacy notice. Make it easy to understand, easy to know what types of data will be collected, easy to know what you're going to do with the data, etc.*

Additional Resources:

Information Commissioner's Office: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/