April 2018

New EU Data Laws

What Not-For-Profit Organizations Need To Know Including Template US/EU Privacy Notice

pillsbury

How will the new European Union data protection law affect U.S. not-for-profit organizations?

Not-for-profit organizations based in the U.S. can often handle large amounts of data which originates in the EU—for example, they may have employees in Europe or a large member database that includes Europeans.

Not-for-profits may receive such data either directly from EU citizens or indirectly including from affiliates or member organizations, acting as a "data controller" with respect to such data (having control over how data is used) or as a "data processor" (acting on the instruction of the party sharing the data).

Unfortunately, being a not-for-profit does not exempt an organization from compliance, which is a common misconception.

The EU General Data Protection Regulation

On 25 May 2018, the EU General Data Protection Regulation 2016/679 (GDPR) will come into force and will apply to any organization, anywhere in the world, which processes the personal data of EU citizens.

As a result, not-for-profit organizations based in the United States that process EU personal data will be required to comply with the GDPR, even though they are based in the United States (or elsewhere outside Europe).

Why is this important?

A failure to comply could attract a fine of up to 20M euros from an EU regulator. Consequences for non-compliance are, therefore, severe.

What are the key changes for not-for-profit organizations?

Some of the key changes introduced by the GDPR include:

- **Data Protection Officers (DPOs).** In many circumstances, controllers and processors will need to appoint DPOs.
- **Data processors.** Where not-for-profit organizations act as a data processor they will have direct liability to EU regulators for the first time if they were to suffer a data breach. They will, therefore, need to audit the data they hold and identify where they are acting as a data processor, including taking steps to protect that data.
- **Consent.** Consent must be "explicit" for certain categories of data collected. Organizations will need to review how data is collected and ensure valid consents are obtained.
- **Privacy policies.** Public-facing privacy policies now need to be more detailed. For example, information needs to be given to individuals about their new enhanced rights to access data and have data about them permanently deleted. Internal policies and processes also need to be updated to handle such requests from individuals.
- **International transfers.** If U.S.-based not-for-profit organizations receive data from within the EU, they will need to consider how those exports/imports are "adequately safeguarded" from an EU perspective. Adequate safeguards need to be put in place with respect to such transfers (e.g., European Commission approved model contract clauses).
- **Breach notification.** New rules requiring data breach reporting within 72 hours (to EU regulators and individuals affected) were enacted through the GDPR. Internal policies and procedures need to be established or updated in order to maintain compliance.
- **Service providers.** Where organizations appoint third parties to carry out services on their behalf and data that originates in the EU is shared with those third parties, then the services contract must contain certain provisions in order to protect the data.

What key actions should be taken done now to prepare?

- **Appoint a Data Processing Officer where required.**
- **Audit your Consents.** Fresh, lawful consents to process data should be obtained where necessary.
- **Review Privacy Notices and Policies.** Outward-facing privacy policies should be updated to ensure compliance with GDPR.
- **Audit imports of data from the EU.** Imports of data should be audited to ensure adequate safeguards are in place.
- **Prepare/Update your Data Security Breach Plan.** Develop a data security breach plan if none is currently in place or update existing plans to reflect the new 72-hour reporting obligations.
- **Set Up an Accountability Framework.** Organizations are required to have a record of all data they process, so an essential step should be to "map" all data currently held by the organization.
- **Review services contracts.** Contracts should be updated to confirm they contain the appropriate data processing and protection clauses required by the GDPR.

Pillsbury Winthrop Shaw Pittman LLP | 1540 Broadway | New York, NY 10036 | 1.877.323.4171
Abu Dhabi o Austin o Beijing o Dubai o Hong Kong o Houston o London o Los Angeles o Miami o Nashville o New York o Northern Virginia o Palm Beach o Sacramento o San Diego o San Diego North County o San Francisco o Shanghai o Silicon Valley o Tokyo o Washington, DC

Template for US/EU Privacy Notice

PILLSBURY NOTE

*A fundamental requirement of the new EU General Data Protection Regulation 2016/679 (**GDPR**), is that your organization must be transparent about how it processes Personal Data.*

There are two elements to this requirement.

First, your organization must understand what Personal Data it holds, where it came from, why you hold it and with whom you share it. In the past, many organizations have not had adequate oversight of their data processing activities and, as a result, will need to undertake a data-mapping exercise to better understand current processes. Certain organizations will also be required to keep up-to-date processing records detailing this information in order to respond to EU regulators, who may request this information without notice.

Secondly, your organization must provide specific information to data subjects about how you process their Personal Data. This information is generally contained in a Privacy Notice or Privacy Policy which must be written in clear and plain language, and should appear in a prominent position on your website. The Privacy Notice should be used in conjunction with an internal Privacy Policy that details how employees should handle Personal Data, how employees should deal with requests from users to access their Personal Data, etc.

This example Privacy Notice, can serve as a helpful starting point to satisfy the requirements of the GDPR and U.S. laws, but must be adapted to reflect how your organization specifically processes Personal Data.

It is important to understand the definition of Personal Data under European law, which in some cases, may be broader than other definitions, such as "personal identifying information" (PII) or "non-public personal information." The definition of Personal Data set out in this draft Privacy Notice mirrors the GDPR.

The example provided below includes drafting notes in gray boxes to help explain each section and identify further considerations for your organization.

ONLINE PRIVACY NOTICE

Effective date: [Date]

Contents

- Who we are
- How to contact us
- How we collect personal data
- Cookies
- "Do not track" signals
- How we use your personal data
- When we share and who can access your personal data
- Selling of your personal data
- Children and privacy
- Security
- Transfer of personal data outside of the European Economic Area (EEA) and international users
- How long we store your personal data

- Where we store your personal data
- Your rights
- Changes to this Privacy Notice
- Information correction, removal, and opting out

Introduction

This Privacy Notice explains how [ORGANIZATION NAME] ("[ORGANIZATION NAME]", "we" or "us") collects and processes your Personal Data. Each time you use our Site, the current version of the Privacy Notice will apply. Accordingly, whenever you use our Site, you should check the date of this Privacy Notice (which appears at the top) and review any changes since the last version. This Privacy Notice is applicable to all Site visitors, registered users, and all other users of our Site.

"**Personal Data**" is any information that enables us to identify you, directly or indirectly, by reference to an identifier such as your name, identification number, location data, online identifier or one or more factors specific to your physical, physiological, genetic, mental, economic, cultural or social identity.

By visiting [www.example.com] or using our mobile application, (together the "Site"), you acknowledge that you have read and understood the processes and policies referred to in this Privacy Notice.

Who we are

PILLSBURY NOTE

Your Privacy Notice should include the full legal name and address of the organization within your group which determines what Personal Data is collected and how it is used (known as, the "Data Controller").

Organizations that provide services or products to data subjects within the EU, but are based outside of the EU, should also provide details of their EU-based representative.

*In some cases, the GDPR may require your organization to appoint a Data Protection Office ("**DPO**"). Where a DPO has been appointed, his or her contact details must be listed in your Privacy Notice.*

For the purposes of the General Data Protection Regulation 2016/679 (the "GDPR"), the Data Controller is [ORGANIZATION NAME] registered in [Jurisdiction] with a registered address at [Address].

[Our nominated representative for the purposes of the GDPR is [Name].]

[Our Data Protection Officer is [Name] who can be contacted by sending an email to [Email address] or by post to [Address].]

How to contact us

PILLSBURY NOTE

Your Privacy Notice should inform data subjects how they can contact you if they have any questions or would like to raise issues with how you are processing Personal Data.

If you have any questions or concerns about this Privacy Notice, please contact us using the Contact Us section on our Site. Alternatively you can contact us by phone at [Telephone number], by sending an email to privacyteam@example.com or by

post to [Address].

How we collect personal data

PILLSBURY NOTE

Your Privacy Notice should set out the ways in which your organization collects Personal Data and any other data that you plan on collecting. It is common practice to divide this section into categories as we have done below.

This section should also notify data subjects of any Personal Data which refers to them, but is received from a third party, e.g. where employers are able to register their employees for individual membership or where Personal Data relating to potential individual members is provided by a marketing company or data broker. The Privacy Notice should be transparent about the relevant procedures and the types of Personal Data shared.

Also, Article 14 of the GDPR requires your organization to notify individuals when their Personal Data is received from a third party within a reasonable period after receiving the Personal Data, but at least within one month. The notification must include, amongst other things, the source of the Personal Data and the purpose for which it is used.

We have included generic data capture points which might apply to most organizations but will need to be explained and adapted in line with your procedures.

Personal Data that you give us

We may collect and process the following Personal Data:

- [**Contact information**]
- [**Membership information**]
- [**Due payment information**]
- [**Purchase information**]
- [**Disciplinary information**]
- [**Certification information**]
- [**Peer review information]**
- [**Medical procedure information**].

Personal data we collect from you

With regard to each of your visits to the Site we will automatically collect the following information:

- [**Technical information**]
- [**Information about your visit**]
- [**Location information**]

Personal data we collect from others

This is information we receive about you if you use any of the other websites (operated by us, or another member of our group) or use any other services provided by another member of our group or us.

Non-Personal Data

We collect information that is sent to us automatically by your web browser and we may use this information to generate

aggregate statistics about visitors to our Site, including, without limitation:

- IP addresses
- Browser type and plug-in details
- Device type (e.g., desktop, laptop, tablet, phone, etc.)
- Operating system
- Local time zone

We may use non-Personal Data for various business purposes such as providing customer service, fraud prevention, market research, and improving our Site. Please check your web browser if you want to learn what information your browser sends or how to change your settings.

Cookies

PILLSBURY NOTE

Under EU law, you must have the consent of the data subject before you are permitted to place cookies and other tracking technologies on a data subject's device, unless the cookie is deemed to be "strictly necessary".

Such consent is obtained, typically, by presenting a visitor with a cookie pop-up on a website home page to inform the user that cookies are in use and to seek the user's opt-in consent for cookies to be placed (depending on how intrusive the cookies are).

Given the strict rules around consent under the GDPR, we would suggest that, where possible, website operators adopt a detailed ***Cookies Policy*** *which is separate from the Privacy Notice so that consent is fully informed and "unambiguous", which is a new requirement under the GDPR.*

Like many websites, our Site uses cookies to distinguish you from other users of the Site. This helps us to analyse the use of the Site to customise and improve the content and the layout of the Site.

When you first access the Site, you will receive a message advising you that cookies are in use. By continuing to browse the Site, you agree to our use of cookies as described in this Privacy Notice.

You do not have to accept our cookies and can block them by activating the setting on your browser that allows you to refuse all or some cookies. You may also delete them after they have been placed on your hard drive. If you do not accept or delete our cookies, some areas of the Site that you access may take more time to work, or may not function properly. For more information about cookies, visit: http://www.allaboutcookies.org.

A cookie is a small file of letters and numbers that we store on your browser or the hard drive of your computer, if you agree. Cookies contain information that is transferred to your computer's hard drive.

We use the following cookies:

- **Strictly necessary cookies**
- **Analytical/performance cookies**
- **Functionality cookies**
- **Targeting cookies**
- **Third-party cookies**

You can find more information about the individual cookies we use and the purposes for which we use them in the table below:

PILLSBURY NOTE

Given the strict rules around consent under the GDPR, it is advisable to list all cookies in use within the Privacy Notice (or separate Cookie Policy), so that consent is fully informed and "unambiguous".

We have included some examples which may be relevant for most organizations.

Cookies used by [ORGANIZATION NAME]

Cookie Source	Cookie Name	Purpose	Expiration
Google Universal Analytics	_ga	This helps us count how many people visit the Site by tracking if you have visited before.	2 years

Third-party cookies used by [ORGANIZATION NAME]

Cookie from	Cookie Name	Purpose
Doubleclick.net	id	Doubleclick is a subsidiary of Google and deals with tailored advertising that is designed to provide you with a selection of products based on what you're viewing on the Site. These adverts are presented to you by Doubleclick when you visit other selected websites—the technology behind the ads is based on cookies. For more information about the Privacy Notice of Doubleclick, please visit: www.google.com/intl/en/policies/privacy/ We'd like to continue to display content that's relevant to you. However, you can choose to opt out of this type of advertising permanently at: https://www.google.com/ads/preferences.

"Do not track" signals

PILLSBURY NOTE

The Online Privacy Protection Act (Cal. Business and Professions Code § 22575) requires that companies specify whether or not they respond to these settings. We have included generic data capture points which might apply to most organizations but will need to be adapted in line with your procedures

[IF THE ORGANIZATION HONORS "DO NOT TRACK" SIGNALS] We support "do not track" signals ("DNT"). If you have DNT enabled in your web browser, we will not receive browser-related information from our advertising partners for tailoring advertisements.

[IF THE ORGANIZATION DOES NOT RESPOND TO "DO NOT TRACK" SIGNALS] We do not respond to web browser "do not track" signals. As such, your navigation of our Site may be tracked as part of the gathering of quantitative user information described above. If you arrive at our Site by way of a link from a third party site that does respond to "do not track" requests, the recognition of any "do not track" request you have initiated will end as soon as you reach our Site.

How we use your personal data

PILLSBURY NOTE

In order to satisfy the transparency principle, the GDPR requires you to identify the reasons why Personal Data is processed within your Privacy Notice. Personal data must not be processed for any purposes beyond those that are contained within the Privacy Notice, or further processed in a manner that is incompatible with those purposes.

The GDPR also requires organizations which undertake "automated decision making" or "profiling" to inform data subjects about the logic

involved in any profiling/automated processing (for example by explaining the data sources and main characteristics of the decision-making process)—this will be particularly important if the result of the profiling produces legal effects or similarly significantly effects, e.g. automatic refusal of an online credit application or online profiling that leads to different individuals being offered different pricing, etc.

Please note that list of potential uses of Personal Data below is generic and will need to be tailored to accurately describe how the Organization uses Personal Data.

We will only process your Personal Data, including sharing it with third parties, where (1) you have provided your consent which can be withdrawn at any time, (2) the processing is necessary for the performance of a contract to which you are a party, (3) we are required by law, (4) processing is required to protect your vital interests or those of another person, or (5) processing is necessary for the purposes of our legitimate commercial interests, except where such interests are overridden by your rights and interests.

We may use Personal Data for the following purposes:

- Personal Data you give to us

We will use this Personal Data:

  - [to carry out our obligations arising from your membership, or any other contract entered into between you and us and to provide you with the information, products and membership services that you request from us;]
  - [to organize events that you have purchased or registered for, and to provide you with information, and other materials, relating to the content of the event, the speakers, sponsors and other attendees;]
  - [to provide our [monthly] newsletter and publication, provided you have given your consent;]
  - [to respond to your questions and provide related membership services;]
  - [to provide you with information about other events, products and services we offer that are similar to those that you have already purchased, provided you have not opted-out of receiving that information;]
  - [to provide you, or permit selected third parties to provide you, with information about events, products or services we feel may interest you, provided you have given your consent;]
  - [to transfer your information as part of a merger or sale of the business;]
  - [to notify you about changes to our membership service; and]
  - [to ensure that content from our Site is presented most effectively for you and your computer.]

- Information we collect about you

We will use this Personal Data:

  - [to administer our Site and for internal operations, including troubleshooting, data analysis, testing, research, statistical and survey purposes;]
  - [to improve our Site to ensure that content is presented most effectively for you and your computer;]
  - [as part of our efforts to keep our Site safe and secure;]
  - [to measure or understand the effectiveness of advertising we serve to you and others, and to deliver relevant advertising to you; and]

- [to make suggestions and recommendations to you and other users of our Site about goods or services that may interest you or them.]

- Personal Data we receive from other sources

We will combine this information with information you give to us and information we collect about you. We will use this information and the combined Personal Data for the purposes set out above (depending on the types of information we receive).

When we share and who can access your personal data

PILLSBURY NOTE

Under the GDPR and U.S. law, your Privacy Notice should include, "the recipients or categories of recipients of the Personal Data, if any". Ideally, your Privacy Notice should identify third parties who will receive Personal Data, and provide links to their privacy policies.

We have included a list of generic categories of third parties which should help you identify the specific third parties with whom Personal Data is shared.

We may share your Personal Data for the purposes described in this Privacy Notice with:

[a member of our group]

[partners, suppliers and sub-contractors]

[analytics and search engine providers that assist us in the improvement and optimization of our Site]

[credit reference agencies]

[trusted third-party companies and individuals]

[in the event that we sell or buy any business or assets, in which case we will disclose your Personal Data to the prospective seller or buyer of such business or assets]

- [if [ORGANIZATION NAME] or substantially all of its assets are acquired by a third party, in which case Personal Data held by it about its customers will be one of the transferred assets.]

PILLSBURY NOTE

Under the GDPR, where your organization shares Personal Data with a third-party vendor, it must enter a data processing agreement which contains specific provision listed in Article 28(3) of the GDPR. These provisions must require the third-party vendor, amongst other things, to only process Personal Data on your documented instructions, to ensure its employees are subject to confidentiality requirements and to implant adequate security measures to protect Personal Data.

We will only transfer your Personal Data to trusted third-parties who provide sufficient guarantees in respect of the technical and organizational security measures governing the processing to be carried out and who can demonstrate a commitment to compliance with those measures.

Selling your personal data

PILLSBURY NOTE

Under the U.S. law, your Privacy Notice should specify whether you plan on selling access to Personal Data. Below, we have included language where an organization may sell access to information and when an organization does not.

[WHEN AN ORGANIZATION MAY SELL ACCESS TO PERSONAL DATA] We will never sell your Personal Data to third parties with whom you do not have an existing relationship. We may sell access to your information (including Personal Data) to our strategic business partners with whom you have an existing relationship in order for our partners to better target their products and services to you. Our partners will not have direct access to your Personal Data but rather will have the ability to communicate with you through your participation with our Site.

[WHEN AN ORGANIZATION WILL NEVER SELL ACCESS TO PERSONAL DATA] We will not sell your Personal Data to third parties for their use without your consent.

Children and privacy

PILLSBURY NOTE

Websites and apps that are designed for children under the age of 13 or collect information from someone under the age of 13, must comply with the Children's Online Privacy Protection Act ("COPPA"). The Children's Online Privacy Protection Rule details the requirements of the Act. The FTC also maintains compliance guidance for COPPA on their Children's Privacy webpage.

Separately, some states in the United States require that minors under the age of 18 have the right to have content and information previously posted to a website or app removed. We have provided some general language that may be need to be modified in accordance with any state-specific laws addressing this topic.

[IF THE ORGANIZATION DOES NOT COLLECT INFORMATION OF CHILDREN UNDER THE AGE OF 13] Our Site is not directed to children under the age of 13, if you are not 13 years or older, do not use our Site. We do not knowingly collect Personal Data from children under the age of 13. If we learn that Personal Data of persons less than 13 years-of-age has been collected through our Site, we will take the appropriate steps to delete this information.

In accordance with [insert state] law, minors under the age of 18 residing in [insert state] may remove or request and obtain removal of content and information that they post on the website or app. In order to remove or to request and obtain removal of such content and information, the user must follow the instructions provided here [insert link].

Security and storage

PILLSBURY NOTE

Under the GDPR and U.S. law, Privacy Notices should generally describe the measures an organization takes to protect against unauthorized access of information, where they are stored, and how information is retained. However, given the widespread prevalence of data breaches it is equally important that the organization also include disclaimers against insuring against the loss, misuse, or unauthorized disclosure of information.

Security

Although we use security measures to help protect your Personal Data against loss, misuse or unauthorized disclosure, we cannot guarantee the security of information transmitted to us over the internet.

Transfer of personal data outside of the European Economic Area ("EEA") and international users

PILLSBURY NOTE

Personal Data relating to European data subjects cannot be transferred outside the EEA (which includes EU countries plus Iceland, Liechtenstein and Norway) without safeguards in place to protect the rights of the data subjects. The concept of "transfer" includes, for

example, a UK subsidiary sharing Personal Data with a U.S. parent company or an organization based in the EU storing Personal Data with a U.S.-based cloud service provider.

Where your organization intends to transfer Personal Data to a third party located outside of the EU, it should identify the third-party recipient, the safeguards which protect that transfer (e.g., standard contract clauses or "MCCs", Binding Corporate Rules, Privacy Shield certification, etc.) and how a data subject can obtain a copy of those safeguards. For example, we have included a reference to a U.S. parent organization and specified standard contractual clauses as the safeguard in place.

Under U.S. law, users of a Site must consent to the transfer of their data, especially Personal Data, outside of the United States if the Site ordinarily stores Personal Data within the United States.

We will not transfer Personal Data, relating to individuals within the European Economic Area ("EEA"), to third parties (i.e., those outside of our group), located outside of the EEA without ensuring adequate protection under European law.

Where a third party is located in a country not recognised by the EU Commission as ensuring an adequate level of protection, we will take appropriate steps, such as implementing standard contractual clauses recognised by the EU Commission, to safeguard your Personal Data.

We will share your Personal Data with members of our group outside of the EEA, including our ultimate holding company [Parent Organization, Inc.] which is based in the United States, for the purposes described in this Privacy Notice. For transfers to [Parent Organization, Inc.], we utilise standard contract clauses recognised by the European Commission. If you would like to obtain a copy of the standard contract clauses, please contact us using the Contact Us section on our Site.

[IF THE ORGANIZATION IS IN THE U.S.] We are headquartered in the United States. Your Personal Data may be accessed by us or transferred to us in the United States or to our affiliates, partners, merchants, or service providers who are located worldwide. If you are visiting our Site from outside the United States, be aware that your information may be transferred to, stored, and processed in the United States where our servers are located, and our central database is operated. By using our Service, you consent to any transfer of this information.

How long we store your personal data

PILLSBURY NOTE

The GDPR requires organizations to specify the period for which the Personal Data will be stored, or if not possible, the criteria used to determine that period. We have, therefore, included a reference to the legal requirement for retention, i.e. no longer than is necessary for the purpose for which the Personal Data is processed. This should be adapted in line with your organization's processes and retention policy.

*This section of the Privacy Notice should work in conjunction with an internal **Data Retention Policy** which sets out the retention periods for various types of data under GDPR and under U.S. law depending on how long an organization retains data.*

*Also, organizations should develop an internal **Deletion Policy** setting out policies and procedures dealing with the destruction of Personal Data, which might be in electronic or physical form (i.e., shredding of documents). The policy should also deal with the decommissioning of assets including software (i.e., outward facing databases) and hardware (i.e., out-of-date devices and servers) which might contain Personal Data and could present a serious security risk if not decommission appropriately.*

We will store your Personal Data, in a form which permits us to identify you, for no longer than is necessary for the purpose for which the Personal Data is processed. We may retain and use your Personal Data as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements and rights, or if it is not technically reasonably feasible to remove it. Consistent with these requirements, we will try to delete your Personal Data quickly upon request.

Retention (U.S. law specific)

[IF THE ORGANIZATION KEEPS DATA ONLY FOR LEGAL PURPOSES] We will retain your information for as long as your account is active or as needed to provide you with our Site. If you wish to cancel your account or request that we no longer use your information to provide you service, contact us at [link]. We will retain and use your information as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements.

[IF THE ORGANIZATION KEEPS DATA INDEFINITELY] We maintain one or more databases to store your Personal Data and may keep such information indefinitely.

Where we store your personal data

PILLSBURY NOTE

The Privacy Notice should specify where Personal Data is stored, i.e., whether on in-house servers, or third-party servers (such as AWS), and should include information about the security measures in place.

Other key internal policies include:

Security Policy

Organization should have robust security policies and procedures concerning the security of Personal Data, and other sensitive information. This should include organizational and technical security measures, such as limiting physical access to Personal Data, a robust password policy, a clean desk policy, a bring-your-own-device security policy, encryption, anonymization and a clear process and responsibility for patching.

Data Breach Policy

The GDPR introduces new rules requiring breach reporting within 72 hours (subject to conditions) where the data breach may result in physical, material or moral damage to an individual. As such, you will be required to have a data breach notification policy in place which meets these new requirements—a European regulator will expect to see this immediately if a breach occurs. Employees must also be trained to recognise a data breach and understand the urgency of reporting this to a manager immediately.

Audit Policy

A policy detailing who in your organization will undertake an audit of the various policies and data processing activities which the organization undertakes. European authorities will expect to see this policy.

All information you provide to us is stored on our secure servers.

[Any payment transactions will be encrypted [using SSL technology].]

Unfortunately, the transmission of information via the internet is not completely secure.

Storage (U.S. law specific)

[IF THE ORGANIZATION stores Personal Data in the United States] The Personal Data that you provide to us is generally stored on servers located in the United States. If you are located in another jurisdiction, you should be aware that once your Personal Data is submitted through our Site, it will be transferred to our servers in the United States and that the United States currently does not have uniform data protection laws in place

Your rights

PILLSBURY NOTE

Under U.S. law, it is customary and typical for Site operators to include procedures to correct and/or remove any information collected

from its users.

In addition, under federal law in the United States, Site users must have the opportunity to opt-out of receiving marketing messages from Site operators.

There are very specific requirements under EU law around user consent to direct marketing sent by electronic means. Broadly speaking, organizations are not permitted to send electronic marketing (including email), unless the recipient has given their prior consent.

Correction and removal

If any of the information that we have about you is incorrect, or you wish to have information (including Personal Data) removed from our records, please contact us at [email].

Opting Out

Additionally, if you prefer not to receive marketing messages from us, please let us know by clicking on the unsubscribe link within any marketing message that you receive, or by sending a message to us at [email].

PILLSBURY NOTE

The Privacy Notice must notify Data Subjects of their rights under the GDPR, as well as their ability to lodge a complaint with a European Data Protection Authority, such as the ICO.

*This section of the Privacy Notice should work in conjunction with an internal **Data Subject Request Policy** which sets out how your organization will respond to data subject who decide to exercise their rights.*

Your European Rights

You have the right to ask us not to process your Personal Data for marketing purposes. We will usually inform you (before collecting your Personal Data) if we intend to use your Personal Data for such purposes or if we intend to disclose your information to any third party for such purposes. You can exercise your right to prevent such processing by checking certain boxes on the forms we use to collect your Personal Data. You can also exercise the right by contacting us using the Contact Us section on our Site.

Under European data protection law, in certain circumstances, you have the right to:

Request access to your Personal Data

Request correction of your Personal Data

Request erasure of your Personal Data

Object to processing of your Personal Data

Request restriction of processing your Personal Data

Request transfer of your Personal Data

- Withdraw your consent

In addition, where you believe that [ORGANIZATION NAME] has not complied with its obligations under this Privacy Notice or European law, you have the right to make a complaint to an EU Data Protection Authority, such as the UK Information Commissioner's Office.

You can exercise any of these rights by contacting us using the Contact Us section on our Site.

PILLSBURY NOTE

California law imposes very specific requirements for Site users residing in California requiring certain businesses to disclose policies relating to sharing certain categories of your Personal Data with third parties.

Your Californian Rights

FOR RESIDENTS OF CALIFORNIA ONLY. Section 1798.83 of the California Civil Code requires select businesses to disclose policies relating to the sharing of certain categories of your Personal Data with third parties. If you reside in California and have provided your Personal Data to Company, you may request information about our disclosures of certain categories of Personal data to third parties for direct marketing purposes. Such requests must be submitted to us at one of the following addresses: [link to email address] or

Company
Attn: California Privacy Rights

_____ [whichever address you want to use]

_____ [whichever address you want to use]

Changes to this Privacy Notice

PILLSBURY NOTE

Under U.S. law, it is customary and typical for Site operators to obtain consent for the continued use of the Site, if the terms of the Privacy Notice change.

If we make any material changes to this Privacy Notice or the way we use, share or collect personal Data, we will notify you by revising the "Effective Date" at the top of this Privacy Notice, prominently posting an announcement of the changes on our Site, or sending an email to the email address you most recently provided us (unless we do not have such an email address) prior to the new policy taking effect.

Any changes we make to our Privacy Notice in the future will be posted on this page and, where appropriate, notification sent to you by e-mail. Please check back frequently to see any updates or changes to this Privacy Notice.

How we can help?

Pillsbury has published a Template Privacy Notice with drafting notes that can be used to assist not-for-profit organizations with the development and revision of your privacy notices to align with GDPR requirements. Our team of professionals can also advise not-for-profit organizations on broader GDPR compliance efforts, including providing specialist input and assistance as required.

Contacts

For further information, contact the following:

Jerry Jacobs, Partner
jerry.jacobs@pillsburylaw.com
Tel: +202.663.8011

Steven Farmer, Counsel
steven.farmer@pillsburylaw.com
Tel: +44.207.847.9526

Meighan O'Reardon, Counsel
meighan.oreardon@pillsburylaw.com
Tel: +202.663.8371