GDPR Compliance Checklist

Last Modified on 06/02/2024 7:26 pm EDT

☐ Identify which users are Data Administrators

Tasks

1. **Define internal policy for which users are identified as Data Administrators**
2. **Identify authorized users as Data Administrators in Application Setup: Users**

Background information:

You can assign any EventsAir user at any level the additional authority to serve as a Data Administrator. This authorization lets the user search for Anonymized records using encrypted name, email or phone numbers from within the Attendee Panel. Data Administrators can also search for encrypted contact details in the Contact Locator.

☐ Archive old events

Tasks

1. **Define internal policy and procedure for when old events are archived**
2. **Archived old events (Located in Edit Event Settings (from the Event Selection Panel)**
3. **Old events are ideally archived before May 25, 2018 (GDPR enforcement date of commencement).**

Background information:

When an event is archived, all attendees are Anonymized and all personal data in the event will be permanently deleted. The attendee's name, email and phone number is permanently encrypted, allowing for a record search only by an authorized Data Administrator.

☐ Identify Fields containing Personal Data

Tasks

1. **Review and identify all fields in current and past events that contain personal data**
2. **Mark appropriate fields by checking the box that states "Contains Personals Data") in the field's setup window**

Background information:

It is important for event managers to review any fields – especially additional fields you have created – so you can mark them as containing personal data if needed. These can be User Defined Contact Fields, Note Types, Marketing Tags and Custom Fields. Identifying any that contain personal data is used by EventsAir for reporting to attendees and when anonymizing or deleting a contact record for data privacy reasons.

☐ Set up default Data Consent policies

Tasks

1. **Discuss and plan what your internal Data Consent Policies should be**
2. **In Application Setup: Offices, enter all Data Consent Policies appropriate to your organization**

Background information:

Data Processing Consent policies are statements shown to a contact prior to them submitting their personal information to you during event registration or using the Attendee App. These statements describe how you plan to use a contact's personal data, including the reasons for collecting their personal data, how long you plan to store their personal data and details of third-party processors accessing their personal data. There are additional policies that need to be defined and these are detailed in the EventsAir and the Data Protection Toolkit White Paper.

☐ Set up Data Consent policies for all active events

Tasks

1. **Review all active events and registration sites**
2. **Apply default consent policies and update as required for each active event**
3. **Update all active registration sites to include the Data Consent component**

Background information:

Even if you have events already in progress, you should add Data Consent Policies in Event Preferences and update all Interactive Sites to display these policies and to capture Consent from new attendees.

☐ Add the Data Protection widget to all user dashboards

Tasks

1. **From each user's Dashboard, select the Data Protection Widget**

Background information:

The Data Protection Widget provides event planners with a snapshot of their Data Protection status across Data Processing Consent, Attendee App Visibility and Compliance. For each category, statistics are displayed, with most of the items having a link that lets you view attendee details or links to Interactive Sites, Apps, Reports and Exports for easy follow up and checking.

☐ Send a Merge Doc to those who haven't given Data Consent

Tasks

1. **Review existing events to determine if you have registered attendees that have not provided Consent**
2. **Create a Merge Doc to send to these attendees and include the Data Processing Consent component**
3. **Search for all attendees that do not have Consent indicated in their contact record**
4. **Send the merge doc to these attendees requesting they check the Consent option within their email**
5. **Using the Data Protection Widget, monitor the response and follow up as needed to capture consent on any remaining attendees without consent indicated in their contact record**

Background information:

If you add Data Consent to an existing event, you may have attendees who have previously registered without indicating consent. This process is important to assure that all contacts in your database have provided consent to using their personal data.

☐ Set (or convert) Quick Reports and Quick Exports to Private

Tasks

1. **Develop internal procedures for when to identify a Quick Report or Quick Export as Private**
2. **Review all existing Quick Reports and Quick Exports and identify which ones should be marked as Private**
3. **When marking a Quick Report or Quick Export as private, also enter the email addresses of third parties authorized to access these reports and exports**

Background information:

It is a requirement to know and manage which third-party processors or individuals are accessing personal data contained in EventsAir, such hotel partners, clients and other service providers. When you create a Quick Report or Export in EventsAir and enable Web Publishing, you can mark these as Private or Public as defined in your organization's policies. This process lets the Data Protection Toolkit track and log every time an authorized third party accesses a Private Quick Report or Export.

☐ Advise third-party data processors of all requests to 'forget' (remove

Personal Data)

Tasks

1. **Develop internal policy and language for advising third party processes when an attendee requests you to remove or "forget" personal data**
2. **Write appropriate language for Third Party Processor communications and enter in both default and event-specific Data Consent Policies**
3. **Whenever you are removing or Anonymizing a contact record, check the box to Advise Third Parties to Remove Personal Data as appropriate to your internal policies**

☐ Add Attendee App Visibility option to all Attendee Apps

Tasks

1. **In Attendee App Setup, add the App Visibility Component and check the box to have the Visibility Option and Opt-In/Opt-Out selection appear automatically if no visibility consent has been provided**

Background information:

Separate from providing Consent to providing personal data for event registrations, attendees also able to Opt In or Opt Out of having their contact details visible in the Attendee App. This allows attendees to attend an event by providing Consent to provide personal data, but Opt Out of having their contact details visible in Attendee Searches, function table allocation and in the EventStream Private Social Network.

☐ Provide a Data Processing Statement to attendees if requested

Tasks

1. **Develop internal policy for responding to Attendee requests to access their personal data, including steps on how to confirm the identity of requesting parties**
2. **Educate your team on the use of the Contact Locator Tool**
3. **Data Administrators can search for attendees by name, review returned records for accuracy and generate a Data Processing Statement to send to the requesting attendee**

Background information:

It is a requirement in GDPR to allow attendees and contacts to request information about what personal data you have as well as how long you plan to use their personal data and what third parties are accessing their information. The Contact Locator Tool that allows you to search for attendee records across multiple events and generate a

detailed Data Processing Statement to send to the requesting party.

It is important to have policies in place for:

– identifying person(s) requesting and approving requests for personal data;

– making sure your team knows how to properly review and select searched contact records in order to generate an accurate Data Processing Statement.

☐ Remove or Anonymize contact records if requested

Tasks

1. **Develop internal policies on determining when to remove or Anonymize a contact record**
2. **Train your internal staff on the correct process when a request to remove "or forget" personal data is received**
3. **When removing or Anonymizing a contact record, remember to check the box informing Third Party Processors of the request (as appropriate to your internal policy)**

Background information:

In terms of protecting the personal data of our attendees you are required to honor a request from an attendee to delete, remove, or "forget" their personal data. However, you also have the right to retain the non-private aspects of the record for reporting and tracking reasons. These could include taxes collected, payments made, registration details, housing reservations and more.

While removing a contact will permanently delete it, EventsAir will not allow you to do so if there are any outstanding financial transactions. It is a common practice for many meeting planners NEVER to delete any record that has financial transactions present, whether they are fully paid or not.

So, when you Anonymize a contact record, you will delete all personal data, encrypt the name, email and phone number, and retain all historical data for reporting reasons.