NOTE: *FIRST* strongly advises organizers of Off-Season Events to consult with an attorney to ensure your consent and release process meets the legal requirements of your local jurisdiction and provides adequate protections for your organization.

Consent and Release Guidance for Off-Season Events - 2024

The *FIRST* Consent and Release Form is designed and optimized for **official** *FIRST* events and season activities. The *FIRST* Consent and Release Form **does not cover** activities that occur outside of our normal program and event structure, such as Off-Season Events.

The sections below describe HQ's approach to collecting consent and release in general terms to help guide the development of your organization's consent process.

The *FIRST* Consent and Release Form has two basic parts. The first part is a **consent to collect personal data (PII)**, and the second part describes the **risks involved with participation in *FIRST* activities** – and the participant's (or parent/guardian of a minor) acceptance of these risks.

Collecting Personal Data (PII)

If you plan to collect personal data to manage your event, including information such as names, phone numbers, email addresses, and photos or video, then you should gain **the affirmative consent** of the data subjects, noting the privacy policy of *your* organization (if available). While the *FIRST* Privacy Policy is not applicable to data collected outside of official *FIRST* systems or processes, your use of personal data **should not conflict with the spirit of the *FIRST* Privacy Policy**. For example, you should not sell, rent, or otherwise share the data of participants for commercial purposes. Please contact the *FIRST* Data Governance Team (Privacy@firstinspires.org) if you have any questions about the types of data you wish to collect, or any concerns about the proposed uses of that data.

The Basic Elements of GDPR-Compliant Affirmative Consent

The section below describes the elements suggested to gain affirmative consent from data subjects to collect and process personal data. **This is provided as a general reference, or best-practice, only; again, *please consult with an attorney when creating your consent requirements.***

- Consent should be **freely given.**
    - A person should not feel pressured into giving consent. If it is not feasible for the person to participate in the event without granting consent or signing a release, there should be no future repercussions. They will simply not be able to participate in the event in question.
    - Minors (under the legal age of majority for the jurisdiction in question) cannot give consent. A parent or legal guardian is the only person who can grant consent for a minor.
- Consent should be the result of **clear affirmative action**.
    - The person must give **express consent** by doing or saying something; in most cases, this means signing an electronic or paper form, or checking a box online.
    - A person cannot give implicit consent by simply ***not*** taking a certain action.
- The text of the consent document or form should be **specific,** and the consent should be **informed.**
    - Explain exactly ***what* personal data you will collect** (e.g., first and last name, email address, date of birth, image, etc.).

- Explain ***how* you will collect, use, and share** personal data, and for how long the data will be **retained**.

- Consent should be **unambiguous.**
    - Consent documents should be in plain language and limit the use of legal or technical terms as much as possible.
- Consent should be **revokable, or able to be withdrawn.**
    - A person who has granted consent for data collection and processing should be able to contact the data controller and withdraw their consent.
    - This withdrawal does not affect the lawfulness of the processing up to that point, it just means you will need to stop any future processing that was based on that consent, ***and, if requested and to the extent feasible***, delete or remove the person's personal data.
    - **There may be a business reason why a person's personal data cannot be completely deleted** – for example, you may need to keep a copy of a signed consent and release form for insurance or legal purposes.

Informing Participants of Risks

It's important to let the people who will attend your event know of any risks related to participation, including injury or illness. The *FIRST* Consent and Release Form describes risks such as physical injury and communicable disease. When creating a consent form for your organization, you should **work with an attorney** and determine the risks you will need to communicate to participants, as well as any requirements you wish to enforce related to a release of liability for injury or illness.

Definitions

Data collection happens when a user deliberately offers or shares personal data – for example when filling out a registration form or when posting a comment on a website.

Data controller refers to an entity that alone or jointly with others determines the purposes and means of the processing of personal data.

Data processing means any operation or set of operations performed upon personal data or sets of personal data, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

A **data subject** a human person who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.

The GDPR, or General Data Protection Regulation, is a law that requires organizations to protect the personal data and privacy of European Union (EU) citizens. *FIRST* and many other US businesses and non-profits that operate in the EU work to the standards of the GDPR, since it provides the highest level of protection for data subjects.

Personal data (also known as personally identifiable information, or PII) is information that can be used on its own or with other information to identify, contact or locate a single person or to identify an individual in context.