INTERPRIDE'S DATA PROTECTION & PRIVACY POLICY

APPROVED JANUARY 2021
TABLE OF CONTENTS

DEFINITIONS
1. DATA PROTECTION PRINCIPLES
2. GENERAL PROVISIONS
3. WHAT INFORMATION DO WE COLLECT?
4. USES OF PERSONAL INFORMATION
5. COOKIES & OTHER TRACKING TECHNOLOGIES
6. SHARING OF INFORMATION
7. LAWFUL, FAIR, AND TRANSPARENT PROCESSING
8. LAWFUL PURPOSES
9. DATA MINIMIZATION
10. ACCURACY
11. ARCHIVING/REMOVAL
12. SECURITY
13. CONFIDENTIALITY
14. BREACH
DEFINITIONS

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>CCPA</td>
<td>California Consumer Privacy Act</td>
</tr>
<tr>
<td>Responsible Person(s)</td>
<td>Methods &amp; Standards Co-Chairs</td>
</tr>
<tr>
<td>Register of Systems</td>
<td>Register of all systems or contexts in which InterPride processes personal data.</td>
</tr>
</tbody>
</table>

1. DATA PROTECTION PRINCIPLES

InterPride is committed to processing data in accordance with its responsibilities under the GDPR, CCPA, and other privacy laws.

Article 5 of the GDPR requires that personal data shall be:

A. Processed lawfully, fairly, and in a transparent manner in relation to individuals;
B. Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be inconsistent with the initial purposes;
C. Adequate, relevant, and limited to what is necessary concerning the purposes for which they are processed;
D. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purposes for which they are processed, are erased or rectified without delay;
E. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to the implementation of the appropriate technical and organizational measures required by the GDPR to safeguard the rights and freedoms of individuals; and
F. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organizational measures.”

2. GENERAL PROVISIONS

A. This policy applies to all personal data processed by InterPride.
B. The Responsible Person(s) shall take responsibility for InterPride’s ongoing compliance with this policy.
C. The Data Controller(s) will include the Co-Presidents, Treasurer, and Vice President of Member Services.
D. This policy shall be reviewed at least annually.
3. WHAT INFORMATION DO WE COLLECT?

InterPride collects personal information that is provided to us directly; such as name, address, contact information, social media, and payment information. InterPride collects passwords, password hints, and similar security information used for authentication and account access. We also obtain personal information from our partners that include but not limited, to the United States Association of Pride (USAP); the European Pride Organisers Association (EPOA); Fierté Canada Pride (FCP); and Consolidated Association of Pride; Inc (CAPI).

4. USES OF PERSONAL INFORMATION

InterPride uses the information we collect or receive:

A. To send information. InterPride uses personal information to send information on our services, events, meetings, community updates, upcoming ballots, training information, and policies’ updates.

B. To manage user accounts. InterPride uses personal information to manage user accounts to keep them in working order.

C. To respond to user inquiries/offer support to users. InterPride may use personal information to respond to inquiries and solve any potential issues members might have.

5. COOKIES & OTHER TRACKING TECHNOLOGIES

InterPride may use cookies and other tracking technologies to collect and store information.

6. SHARING OF INFORMATION

InterPride may process or share data based on the following basis:

A. Consent: Process data if given specific consent to use personal information for a specific purpose.

B. Legitimate Interests: Process data when it is reasonably necessary to achieve our operational goals.

C. Legal Obligations: Disclose information where we are legally required to do so to comply with applicable law, governmental requests, a judicial proceeding, court order, or legal processes, such as in response to a court order or a subpoena (including in response to public authorities to meet national security or law enforcement requirements).

D. Vital Interests: Disclose information where it is necessary to investigate, prevent, or take action regarding potential violations of our policies, suspected fraud, situations involving potential threats to the safety of any person and illegal activities, or as evidence in litigation in which we are involved.

E. Vendors, Consultants, and Other Third-Party Service Providers: Share data with third-party vendors, service providers, contractors, or agents who perform services for us or on our behalf and require access to such information to do that work. Examples include payment processing, data analysis, email delivery, hosting services, customer service, and marketing efforts.

InterPride is committed to only sharing data with bodies which have the same or higher level of data protection policy AND are located in the United States, Canada, or the European Union. Unless explicit consent is obtained, InterPride does not share, sell, rent, or trade any personal information with third parties for their promotional purposes.
7. LAWFUL, FAIR, AND TRANSPARENT PROCESSING
   A. To ensure its data processing is lawful, fair, and transparent, InterPride shall maintain a Register of Systems.
   B. The Register of Systems includes YourMembership, Google Groups, and Slack.
   C. The Register of Systems shall be reviewed at least annually.
   D. Individuals have the right to access their personal data, and any such requests made to InterPride shall be dealt with promptly.

8. LAWFUL PURPOSES
   A. All data processed by InterPride must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task, or legitimate interests.
   B. InterPride shall note the appropriate lawful basis in the Register of Systems.
   C. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
   D. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available, and systems should be in place to ensure such revocation is reflected accurately in InterPride's systems.

9. DATA MINIMIZATION
InterPride shall ensure that personal data are adequate, relevant, and limited to what is necessary in relation to the purposes they are processed using YourMembership, Google, and Slack.

10. ACCURACY
   A. InterPride shall take reasonable steps to ensure personal data is accurate.
   B. Where necessary for the lawful basis on which data is processed, steps shall be taken to ensure that personal data is kept up to date.

11. ARCHIVING/REMOVAL
   A. To ensure that personal data is kept for no longer than necessary, InterPride shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
   B. The archiving policy shall consider what data should/must be retained, for how long, and why.
   C. Any person contacting InterPride can request a copy of their data, and that data will be provided within 14 days, and that they can request its removal also within 14 days.
12. SECURITY

A. InterPride shall ensure that personal data is stored securely using modern software that is kept-up-to-date.

B. Access to personal data shall be limited to personnel who need access, and appropriate security should be in place to avoid unauthorized information sharing.

C. When personal data is deleted, this should be done safely such that the data is irrecoverable.

D. Appropriate back-up and disaster recovery solutions shall be in place.

13. CONFIDENTIALITY

All Board, Global Advisory Council, and Committee Members of InterPride, including the Chairs, are authorized to have access to personal data; only to the extent necessary to perform the responsibilities of their positions. Personal data includes, but is not limited to, name, address, phone number, email and financial information. They are legally bound to safeguard personal information and MUST not share such data with others that are not authorized, or have not signed a data confidentiality agreement. This obligation of confidentiality shall survive after their term in office or service to the organization's end.

14. BREACH

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data; InterPride shall promptly assess the risk to people’s rights and freedoms and, if appropriate, report this breach to the relevant authorities.