Membership Data Governance Policy

Prepared by the Membership Committee and

Membership Services Officer August 2020

Next Review Due August 2023

Introduction

The Society for Industrial-Organizational Psychology (SIOP) is made up of approximately 10,000 members[1]; understanding their composition is critical to guiding executive and committee decisions pertaining to membership recruitment, retention, events, benefits, policies, and more. The Membership Analytics Subcommittee (MAS), a subset of SIOP's Membership Committee, was formed to analyze membership data and provide insights to aid in decision making. By leveraging SIOP's extensive database of membership information, SIOP leaders can make informed decisions that reflect an accurate understanding of the current state of SIOP membership. Equally important is the protection of private membership information. Therefore, analysis and use of membership data[2] requires policy to govern access, storage, and reporting.

Data governance is a cross-functional management activity that, at its core, recognizes data as an enterprise asset. This policy is meant to ensure (1) that membership data are treated as an asset, which are protected and managed as such and (2) that data are stored, shared, used, and reported in a responsible and ethical manner.

Provided below are some common uses of membership data for the purposes of informing SIOP leaders and members:

- Provide snapshots of SIOP membership demographics and trends in the form of membership reports

[1] For the purposes of these guidelines, any dues-paying individual making up one of the membership categories described at https://www.siop.org/Membership/Criteria is covered under the term "SIOP member."
[2] Membership data includes all profile and membership status information provided by potential members during the application process and/or as part of attendance at SIOP events as well as that of former SIOP members whose membership status may have lapsed and non-member customers.

- Routinely provide additional custom reports that drive action items for the Membership Committee
- Provide a summary and initial recommendations following monthly updates on annual membership trends

The following document will outline guidance for analysis, storage, and sharing of membership data and insights particularly as it pertains to the responsibilities of SIOP's MAS. The sections of the policy include:

Section 1: Membership Data Governed by This Policy

While there are other sources of data within SIOP (e.g., SIOP surveys, web page analytics), this policy is focused specifically on data that describe SIOP members and/or pertain to SIOP membership, which include the following sources:

- All online profile information (i.e., information provided by potential members upon application as well as information provided by current or past members in their online member profiles), including but not limited to the following demographic characteristics: birthdate, gender, mailing address, ethnicity, degree, year graduated, employer type, interests, certifications, and other pertinent information
- Membership dues information detailing when and what types of membership dues payments are made by each member (e.g., associate membership payment)
- Membership tenure (i.e., the number of years an individual has been a member of SIOP which is calculated based on original join date and all years of active membership)
- SIOP's event and program data, including SIOP member and nonmember event attendee demographics, event and program metrics (e.g., sessions attendance, participation in conference related programs, such as the Membership Ambassador Program), event submissions information, and other SIOP program participation (e.g., research access subscribers)

The values that govern the use of this data relate to data privacy, security, maintenance, and accessibility to those who would utilize it for the improvement of member experiences within SIOP. Specifically, as it pertains to member privacy, usage of any data considered personally identifiable information (PII) by the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) regulations must adhere to those regulations. SIOP's

policy is to ensure all member data are secure, protected, and maintained in accordance with GDPR and CCPA. Additional details are included in the Appendix. The following sections detail policies and procedures enacted to ensure these values are upheld.

Section 2: Member Data Governance Policies and Guidelines

The MAS was formed to bridge a gap by providing access to membership trends and insights to improve SIOP member experiences and inform leadership decisions. Responsibilities of the subcommittee include:

- Review and respond to requests for membership information
- Report on membership trends regularly
- Publicize deidentified member information for the benefit of SIOP members
- Incorporate new data on a semi-annual basis as it is made available
- Communicate with the Administrative Office and Executive Board regarding results from analysis
- Provide recommendations for future data requirements to inform membership decisions, including recommendations on the collection and systems that store such data
- Protect and maintain member privacy.

Guidelines to govern MAS access, storage, analysis, and reporting of membership data are provided below. While these guidelines are generally focused on the responsibilities of the MAS, they may be helpful for SIOP leadership, committees, and members who seek to understand potential uses and limitations of membership data.

Access and Storage.

In order to maintain members' privacy rights, access to individual level membership data is restricted. Direct access to the full membership database is limited to SIOP's Administrative Office (AO)[3]. Upon request (typically on a bi-annual basis), SIOP's AO provides the MAS with

[3] Members have direct access to individual level member data through the membership directory and various committees have access to other types of membership data by virtue of their work (e.g., SIOP's Awards Committee

access to specific membership data files, ensuring that the only individually identifiable information shared is the SIOP ID (SID)[4], an identifying variable created by the AO to match member data across time[5]. This access is provided by uploading password protected files to a secure, cloud storage drive (i.e., Dropbox) that is only accessible to current members of the MAS and the AO, with specific permissions restricted based on MAS role (e.g., editing, viewing, sharing, etc.). These files are maintained and accessed through the cloud storage drive; files should never be stored on an individual MAS members' computer or device. At the end of each SIOP membership year, access will be reviewed and removed for all members transitioning off the MAS.

All requests for membership data from individuals not working in the AO should be routed through the MAS in order to ensure adherence to this data governance policy. Raw, individual level membership data cannot be provided outside of the MAS -- it is the responsibility of the subcommittee to perform analyses to summarize individual level data and provide timely answers to membership questions.

To that end, any SIOP member may submit a request for membership information[6]. Requests will be prioritized, such that requests from the Executive Board are fulfilled first, with other requests being processed in this order: requests from the AO[7], requests from Committee Chairs, requests from Committee members, then requests from individual SIOP members. Decisions regarding whether or not to fulfill a request will depend on the potential value and use

has access to member CVs and the Program Committee has access to conference submissions); however access to the database containing all membership data is limited to the AO.

[4] SID is required to enable the tracking of membership trends over time and across data sources.

[5] Only the AO is granted access to the key mapping members to SID.

[6] If nonmembers make requests, those requests will be reviewed by the membership committee chair for further direction.

[7] The AO may make requests for advanced analyses that aren't available within the capabilities of their reporting platform.

of the information requested, as reported during the request process. The process for requesting this access is detailed in Section 3 of this document.

Analysis and Reporting.

There are a diverse range of demographic variables within SIOP membership (e.g., ethnicity, degree type, location, membership type, etc.). To the extent that it is valuable for understanding membership trends and/or answering specific membership questions, MAS analyses will seek to retain as much granularity in membership categories and subgroups as possible before being collapsed into more broad categories. At minimum for basic demographic reporting, there must be at least 10 members within a subcategory in order to report membership data for that group[8]. While the minimum subgroup sample size is 10, depending on the type of analysis, the MAS will refer to the typical sample size requirements given by the standards of running that particular analysis and adjust that minimum upwards where power analyses and/or convention imply the need for a larger minimum.

Finally, where possible and to the benefit of SIOP membership as a whole, the MAS will utilize SIOP publication outlets (e.g., Newsbriefs, *The Industrial-Organizational Psychologist*) to share the results of membership analyses broadly, with the goal of allowing all members to benefit from the combined power of their membership data. Requests for membership analyses should detail how or if they intend to share the results with any audience beyond themselves.

[8] This minimum is consistent with other SIOP reporting conventions, including SIOP's Research Guidelines and Policies for Member Surveys.

Section 3: Request and Approval Process

Step 1. Submit Membership Data Request.

Any SIOP member or AO staff member[9] seeking information about membership characteristics or trends may submit a request using the online form available here. Each of the following should be detailed within the request:

- The scope of the request, including the membership characteristics about which you are interested in learning more.
- The goals of the request, including its intended use or application.
- The timeframe within which the requested analyses are needed.
- A description of how the results of the analyses will benefit SIOP members.
- A description of the individuals or groups to whom the results will be made available, especially if they will be shared beyond the requester(s).

Note, the MAS will confirm receipt of materials upon submission.

Step 2. MAS reviews request.

The MAS chair(s) will then review the request and communicate their decision to approve or deny the request based on the following criteria:

- Priority level, which will be determined through a combination of the requestor's purpose, group represented (e.g., the Executive Board, SIOP committee), and defined timeframe.
- Feasibility, which will be determined by examining the potential to provide insights given limitations in the data. The request will typically be deemed feasible if (1) variables

[9] The AO may make requests for advanced analyses that aren't available within the capabilities of their reporting platform.

exist to answer the requester's questions, (2) the variables are not subject to data integrity issues, such as large amounts of missing data, and (3) the resources required to fulfill the request can be allocated to the task based on the time needed to clean, manipulate, and analyze the requested membership data.

- Potential benefit, which will be determined by examining the possibility of the analyses to inform SIOP policies, procedures, and decisions to improve member experience.
- Ethical considerations, including the potential for the specific combinations of data requested to impact privacy as well as the potential for misuse of the results.

Note, in some cases, a request may receive partial approval based on feasibility and other factors.

Step 3. If approved, the request is fulfilled.

Once approved, the request will be assigned to one or more MAS members who will process the request, reaching out directly to the requestor with any specific follow up items. Once the request is processed, the MAS chair(s) will review the output for accuracy before it is released to the requester. Where relevant to a broader audience, the MAS may release findings through one or more of SIOP's communication channels (e.g., SIOP Newsbriefs).

Appendix

Privacy Laws Impacting SIOP Data Use

SIOP Privacy Policy

The SIOP Privacy Policy may be found at: https://www.siop.org/Privacy-Policy

EU Data Rights

On May 25, 2018, the European Union's ("EU") General Data Protection Regulation ("GDPR") went into effect. In accordance with the GDPR, identifiable natural persons ("data subjects") located within the EU must be provided with the following information:

Contact Details of Controller:

Society for Industrial and Organizational Psychology 440 E. Poe Rd. #101, Bowling Green, Ohio 43402

Purposes of Processing:

Personal data are processed for the purposes set forth in this Privacy Policy. The legal basis for the processing activities detailed in this document is by consent and contract as detailed in this Privacy Policy. Recipients or categories of recipients of the personal data: Personal data are received by our payment card service provider for the sole purposes of processing payment transactions on our Sites. Personal data is also received by our trusted third party business partners, who provide us with data and platform hosting services, by contract.

Personal Data Storage Criteria:

Personal data is stored by us until such time as you contact us in writing to request that your personal data be deleted.

Data Rights:

EU data subjects have the following data rights:

- Right to access to the personal data we have for such data subject;
- Right to rectification of incorrect personal data;
- Right to erasure of the personal data we have for such data subject;
- Right to restriction of processing concerning such data subject;
- Right to object to our processing of such personal data;
- Right to data portability, that is, a copy of the data we have on such data subject;
- Right to withdraw consent at any time to our processing of such data subject's personal data; and
- Right to lodge a complaint with a supervisory authority.

You may exercise your data rights by contacting us, in writing, at the address indicated above.

The California Consumer Privacy Act (CCPA)

The California Consumer Privacy Act (CCPA) was enacted in 2018 and took effect on January 1, 2020. This landmark piece of legislation secured new privacy rights for California consumers. On October 10, 2019, Attorney General Xavier Becerra released draft regulations under the CCPA for public comment.

The CCPA grants new rights to California consumers

- The right to know what personal information is collected, used, shared or sold, both as to the categories and specific pieces of personal information;
- The right to delete personal information held by businesses and by extension, a business's service provider;
- The right to opt-out of sale of personal information. Consumers are able to direct a business that sells personal information to stop selling that information. Children under

the age of 16 must provide opt in consent, with a parent or guardian consenting for children under 13.

- The right to non-discrimination in terms of price or service when a consumer exercises a privacy right under CCPA.