International Consortium of
PLAY THERAPY ASSOCIATIONS

Integrity • Quality

IC-PTA Data Protection Policy and Privacy Statement

Adopted by Board of Directors, 27 September 2023

This covers:
1. Data Protection;
2. Data Access Requests;
3. Data Breach Notification;
4. Website Privacy;
5. Management of email mailing list.

1. Data Protection Statement.

This Data Protection Policy provides information about which personal data is recorded by IC-PTA (International Consortium of Play Therapy Associations) and how, where and for what purpose it is processed. The protection of personal data is very important to the IC-PTA and to this end the relevant regulations are observed.

The following data protection policy applies to all persons whose personal data are processed and also applies to users of our website and newsletter recipients.

The activities of IC-PTA are subject to Swiss data protection law.

1.1 Purpose.

To demonstrate compliance with the Data Protection principles set out in Switzerland's Data Protection Act 2022 (nLPD).

1.2 Scope.

This Policy applies to all Personal Data collected, processed and stored by IC-PTA.

1.3 Responsibility.

The IC-PTA Board of Directors hold overall responsibility and are responsible for compliance. The Board elects an individual who acts as Data Protection contact.

2. Data Protection Processing.

2.1 Definition.

Personal data is defined as any information about a specified or determinable person. The data subject is the person whose personal data are processed. Processing includes any processing of personal data, irrespective of the means and methods used, in particular storage, disclosure, obtaining, acquisition, erasure, storage, modification, destruction, and use of personal data.

2.2 Legal Bases.

The International Consortium of Play Therapy Associations (IC-PTA) is committed to complying with the Data Protection Act 2022 which comes into force in Switzerland on 1st September 2023 and, where applicable, the Data Protection principles set out in the General Data Protection Regulation 2016/679 (GDPR).

IC-PTA process personal data in accordance with Swiss data protection law, in particular the Federal Data Protection Act (DPA) and the Ordinance on the Federal Data Protection Act (DPA).

We process personal data - if and to the extent that the General Data Protection Regulation (GDPR) is applicable - in accordance with at least one of the following legal bases:

6 para. 1a GDPR: for processing personal data with the consent of the data subject.

6 para. 1b GDPR: for the necessary processing of personal data for the performance of a contract with the organization concerned.

6 para. 1f GDPR: for the necessary processing of personal data for the protection of our own or third parties' legitimate interests, unless the freedoms, rights and fundamental interests of the data subject prevail. Legitimate interests are in particular our interest in being able to provide the agreed services.

6 para. 1e GDPR: for the necessary processing of personal data for the performance of a task in the public interest.

This Policy applies to all Personal Data collected, processed and stored by IC-PTA in relation to its members, Board of Directors and full time or part-time, employed or self-employed staff. All are treated equally under this policy. The policy applies equally to personal data held in manual and automated form. All Personal Data will be treated with equal care by IC-PTA.

2.3 IC-PTA as a Data Controller.

As part of its daily organisational activities, IC-PTA acquires, processes, and stores personal data in relation to:

- Operating Member Organisations, including personal details of Operating Member representatives;
- Individual Members;
- Organisational Members including personal details of named contact persons;
- Founding Members;
- Honorary Members;
- Contracted persons or persons representing contracted organizations.

2.3.1 Security.

We process personal data necessary to provide our services in a permanent, secure and reliable manner. Such personal data may fall into the categories of constituent and contact data and browser data. Bank account details may be used for membership payment, credits, and refunds.

This data must be acquired and managed fairly. We process personal data for the period of time necessary for the corresponding purpose(s) or as required by law. Personal data whose processing is no longer necessary are anonymized or deleted. The individuals whose data we process have the right to request the modification or deletion of their data, which will be final once the data backup period has elapsed (maximum 6 months).

2.3.2 Consent.

We process personal data only with the consent of the data subject, unless processing is permitted for other legal reasons (such as to fulfil a contract with the data subject).
In this context, we specifically process information that a data subject voluntarily and personally transmits to us when they contact us-for example, by mail, e-mail, social media, or telephone, or when they make their contact information available in connection with an organisation. We also process personal data that we receive from third parties, obtain from publicly accessible sources, or collect in the course of providing our services, if and to the extent that such processing is permitted by law.

2.3.3 Storage.

Such information may be recorded in an address book, in a CRM (Customer Relationship Management) system or with similar tools. When a user transmits personal data relating to third parties to us, he or she will be required to ensure data protection with respect to such third parties and to ensure the accuracy of such transmitted personal data. Personal data transmitted to IC-PTA will not be forwarded externally without the prior consent of the data subject.

2.4 Processing of personal data by third parties, including abroad.

As an international organisation IC-PTA may use third-party services for the operation of some services, and for this reason, we may engage third parties to collect personal data and process them. We ensure adequate data protection of these services even if they are not based in Switzerland or Europe. Exceptionally, such third parties may be located in a country that does not have adequate data protection, and IC-PTA will ensure that data protection requirements are met according to this policy.

2.5 Use of images.

Nowadays, Swiss law does not include any article on the "Right to one's own image." However, each person has the right to decide whether to actually use images that represent him or her and in what context. With this in mind, during the events it organizes, IC-PTA will ask people in attendance to sign a "Release for the Use of Personal Images" and will refrain from photographically portraying people who do not sign it.

The images will then be recorded in the IC-PTA Databases and possibly published on the IC-PTA website or its Social Media pages.
However, IC-PTA will allow itself to use images portraying people taken during events and demonstrations provided that the person or persons depicted are not highlighted, but rather perceived as belonging to the group of people. In such cases, there is no infringement of the right.

3. Rights of data subjects.

Data subjects whose personal data IC-PTA processes enjoy the rights provided by the Swiss Data Protection Act. They include the right to information as well as the right to rectification, erasure or blocking of processed personal data.

3.1 Data deletion and retention period.

Recorded personal data will be deleted as soon as the purpose for which it was stored is no longer valid. You can request the deletion of your personal data by sending an email to info.icpta@gmail.com . The final deletion of data takes place when the prescribed retention periods expire (maximum 6 months). However, these may be extended for any official reasons.

3.2 Data storage and security

Your data are treated confidentially. We use appropriate technical and organizational precautions to protect data from loss and manipulation and from unauthorized access by third parties (i.e. periodically changed passwords, double identification).

3.3 Automated decision-making in individual cases, including profiling.

No automated decisions are made in the processing of personal data and no profiling is performed.

3.4 External links indicated on the website. www.ic-pta.com

This data protection policy does not apply to websites that can be accessed via a link on the IC-PTA website. IC-PTA therefore assumes no responsibility in this regard; please refer to the data protection declaration of the website in question.

4. Databases used and location of servers.

I C-PTA uses third-party services to provide services in a permanent, secure and reliable manner. To enable its team to collaborate securely, IC-PTA registers its working documents on the Dropbox Database, on servers based in Europe. This service complies with GDPR standards and is committed to ensuring the security and protection of its users' data at all times in line with legal requirements and best practices. In accordance with its commitment to users, Dropbox is working hard to ensure Dropbox's compliance with GDPR (including the appointment of a data protection officer, reorganization of the privacy program to ensure that users can exercise their rights as data owners, documentation of data processing activities, and strengthening of internal processes in case of security breaches. Dropbox continues to make changes to ensure that as data protection authorities publish new guidelines, processes and practices comply with or exceed specific components of the new rules). For more information:
https://help.dropbox.com/it-it/security/general-data-protection-regulation

IC-PTA Board of Directors utilise Slack Technologies https://slack.com/intl/en-gb/ for day to day business and internal communication. The Slack Privacy Policy https://slack.com/intl/en-gb/trust/privacy/privacy-policy describes how Slack collects, uses and discloses information associated with an identified or identifiable individual (referred to in this Privacy Policy as **'Personal Data'**) and what choices IC-PTA have around this activity. This service complies with Californian data protection law and GDPR standards and is committed to ensuring the security and protection of its users' data at all times in line with international legal requirements and best practices.

4.1 Data Security.

We take congruent and appropriate technical and organizational measures to ensure the protection and in particular the security of data. However, despite these measures, the processing of personal data on the Internet may always have security gaps. Therefore, we cannot guarantee absolute data security.

4.1.1 IC-PTA database security.

IC-PTA uses Dropbox services to record its working documents on European servers. To maintain a high level of security, Dropbox has developed multiple layers of protection:

- Dropbox files stored are encrypted with 256-bit AES (Advanced Encryption Standard).
- To protect data in transit between Dropbox apps and servers, Dropbox uses Secure Sockets Layer (SSL)/Transport Layer Security (TLS) technology. This SSL/TSL technology creates a secure tunnel protected by 128-bit or higher Advanced Encryption Standard (AES) encryption. • Dropbox applications and infrastructure are periodically tested for

vulnerabilities and constantly enhanced to increase security and protect them from attacks

- Two-step verification is performed when users log in for an additional layer of security
- Public files are visible only to people with the relevant links

IC-PTA Board use Slack to manage day to day business communication and to temporarily store documents e.g. reports, minutes and agendas. Slack takes security of data very seriously. Slack works hard to protect Information that IC-PTA provides from loss, misuse and unauthorised access or disclosure. These steps take into account the sensitivity of the information that we collect, process and store, and the current state of technology. Slack has received internationally recognised security certifications. To learn more about current practices and policies regarding security and confidentiality of the Services, please visit our Security practices. Given the nature of communications and information processing technology, Slack cannot guarantee that Information during transmission through the Internet or while stored on our systems or otherwise in our care will be absolutely safe from intrusion by others. When you click a link to a third-party site, you will be leaving our site, and we don't control or endorse what is on third-party sites.

5.1 IC-PTA website security.

Access to the www.ic-pta.com website is through transfer encryption (SSL/TLS, specifically with Hypertext Transfer Protocol Secure, abbreviated HTTPS).
We use the services of third parties in order to take advantage of the digital infrastructure required for our services. These include in particular the hosting and storage services provided by Wix.com. These providers may process - usually exclusively on our behalf - the data necessary for operation from the website. This includes in particular your IP (Internet Protocol) address. We ensure adequate data protection with such service providers.

5.2 Usage Data

To analyze the usage of the www.ic-pta.com website we use the services provided by Wix.com; an online platform that allows to measure the reach of different pages on the website in an anonymous way. Learn more about privacy and security here: https://www.wix.com/manage/privacy-security-hub/faq and https://www.wix.com/about/privacy. The data collected allows us to improve the quality of service based on the recognition of trends and user behaviour. All site measurements are done anonymously.

5.3 Use of Functional Cookies

The www.ic-pta.com website uses functional cookies but no tracking cookies and no personal data is collected. Cookies are data in text form that are stored in the user's browser. Cookies cannot run programs or transmit malicious software such as trojans and viruses. As mentioned in Section 5.1, the IC-PTA website uses Wix.com services to perform the analysis of the usage data of the same. We have included on the website the option for users not to accept cookies.

5.4 Data collection during registration processes.

Membership application to IC-PTA requires the entry and involves the registration of certain personal data. Data will not be passed on to third parties.

5.5 Data processing for registration on the mailing list.

From the website www.ic-pta.com it will be possible to register to receive IC-PTA's informative twice yearly newsletter.

At any time, you can unsubscribe from the mailing list by clicking the link at the end of any newsletter. The email address will then be permanently deleted from the subscription list.

6. Use of personal data in communications.

6.1 Consent and objection.

By becoming a member of IC-PTA you consent to the use of your e-mail address to inform you about membership and related issues, to receive the newsletter and to answer any queries. You can unsubscribe from notifications and communications such as newsletters at any time. We reserve the right to send notifications and communications absolutely necessary for our business to a personal email, general address of the organization, or if so expressly indicated to a personal email indicated by the organization in question.

If a member of the public sends a query by email, the administrator will reply to answer the question. Thereafter the email address will not be used for any correspondence from IC-PTA that has not been requested and this email address will not be added to IC-PTA mailing list.

6.2 Measuring success and the number of users reached.

Emails and communications may contain links or counting pixels that record in a totally anonymous way whether an individual message was opened and which links were clicked. We need this statistical record of usage to quantify interest and the number of users reached in order to offer notifications and communications based on the needs and reading habits of recipients.

7. Social media.

We are present on social media platforms to communicate with interested persons and to inform them about our activities. The processing of personal data may also take place outside Switzerland and the European Economic Area (EEA).

The General Terms and Conditions (GC) and Terms of Use, as well as the data protection declarations and other provisions of the individual operators of these online platforms also apply in each case. These provisions provide information in particular on the rights of data subjects, including in particular the right to access information.

[TO BE UPDATED: List Social media accounts here with links to their data protection and privacy:]

8. Managing a data breach.

See Appendix 1. "IC-PTA Information Management: Data Breach Notification"

8.1 General disclaimer.

All of the above information has been carefully checked and IC-PTA undertakes to ensure that it is up-to-date, correct and complete as far as possible. However, the occurrence of errors cannot be completely excluded, and claims for damages caused by the use of the information provided, including incomplete or incorrect information, will therefore be rejected.

However, the user always has the right to revoke the consent given for the use of his or her personal data at any time.

The IC-PTA editors may change or delete text at their own discretion and without prior notice and are not obliged to update the contents of the website www.ic-pta.com. Use of and access to the website is the responsibility of the user. The editors are not responsible for any

damages, such as direct, indirect, incidental, or consequential damages, alleged to be caused by the use of this website and accordingly assumes no liability for such damages.

The editors also assume no responsibility for the content and availability of third-party Web sites that may be accessed through external links on this site. The operators of the linked sites are solely responsible for their content. The editors therefore expressly distance themselves from all third-party content that may be relevant to criminal law or civil liability or that may offend public decency.

9. Reservation of the right to amend.

IC-PTA reserve the right to amend or supplement this policy at any time at our sole discretion and in accordance with data protection legislation. Therefore, please consult regularly the policy found at www.ic-pta.com.

Appendix 1.

"IC-PTA Information Management: Data Breach Notification"

1. Introduction. **1.1 Purpose** The purpose is to demonstrate compliance with the obligations of a Data Controller under Swiss Data Protection Law and GDPR in regard to notification of any data breach.

1.2 Scope This procedure applies to any personal data breach within IC-PTA and the notification of such a breach to the Swiss Federation EDOAB and to the subject in the relevant circumstances.

1.3 Responsibility The Data Protection Contact

2. Data Breach Notification Policy.

IC-PTA policy on Data Breach Notification is to comply with the obligations of a Data Controller under Swiss Data Protection Law and GDPR.

There are two primary obligations;

- notification of any personal data breach to the Swiss Federation EDOAB unless they can demonstrate it is unlikely to result in a risk to data subjects;
- communication of that breach to data subjects, where the breach is likely to result in a high risk to data subjects.

The Data Controller must also ensure, in line with the accountability principle set out in Article 5(2) GDPR, as well as the requirements of Article 33(5), that they document any and all personal data breaches, including the facts relating to the personal data breach, its effects and the remedial action(s) taken which will enable them to demonstrate compliance with the data breach notification regime to the Swiss Federation EDOAB.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

'Personal Data' means any information concerning or relating to an identified or identifiable individual.

Personal data breaches include incidents that are the result of both accidents (such as sending an email to the wrong recipient) as well as deliberate acts (such as phishing attacks to gain access to customer data). A personal data breach occurs in incidents where personal data are lost, destroyed, corrupted, or illegitimately disclosed. This includes situations such as

where someone accesses personal data or passes them on without proper authorisation, or where personal data are rendered unavailable through encryption by ransomware, or accidental loss or destruction.

A personal data breach is a security incident that negatively impacts the confidentiality, integrity, or availability of personal data such that the Data Controller is unable to ensure compliance with the principles relating to the processing of personal data as outlined in Article 5 GDPR.

All personal data breaches are security incidents, not all security incidents are necessarily personal data breaches.

The Data Controller is obliged to notify the Swiss Federation EDOAB of any personal data breach that has occurred, unless they are able to demonstrate that the personal data breach is 'unlikely to result in a risk to the rights and freedoms of natural persons' where the controller has assessed the breach as unlikely to present any risk to data subjects and can show why they reached this conclusion. In any event, for all breaches – even those that are not notified to the Swiss Federation EDOAB, on the basis that they have been assessed as being unlikely to result in a risk – controllers must record at least the basic details of the breach, the assessment thereof, its effects, and the steps taken in response, as required by Article 33(5) GDPR.

3. Data Breach Notification Procedure

Any IC-PTA member or third party who suspects that a data breach may have occurred reports the incident to the IC-PTA Data Controller by email: info.icpta@gmail.com

The initial report should describe the nature of the incident, including, where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned.

Assessment

The Data Controller will record:

- how and when they became aware of reported personal data breaches;
- how they assessed the potential risk posed;
- determine whether a breach has occurred and how serious the breach is on affected individuals taking into account the impact the breach could potentially have on individuals whose data has been exposed;
- record the basic details of the breach/incident, the assessment thereof, its effects, and the steps taken in response even if the breach is not considered reportable.

The Data Controller will consider the nature of the breach, the cause of the breach, the type of data exposed, if there are mitigating factors in place, and whether the personal data of vulnerable individuals has been exposed. The levels of risk are defined below:

- Low Risk: The breach is unlikely to have an impact on individuals, or the impact is likely to be minimal.
- Medium Risk: The breach may have an impact on individuals, but the impact is unlikely to be substantial.
- High Risk: The breach may have a considerable impact on affected individuals.
- Severe Risk: The breach may have a critical, extensive or dangerous impact on affected individuals.