Statement of the Board of the Austrian Physical Society (OePG) on Privacy Policy

(Passed at the board meeting on May 22, 2018)

1. Preamble

In order to fulfil its responsibilities, the Austrian Physical Society (OePG) has to collect and process certain data, including individual-related data. The protection of this data is a matter of highest importance for the OePG. With the exception of the exhaustive list of cases defined below, person-related data must not be passed on to anyone inside or outside the Society. With very few exceptions, the OePG collects itself the data listed below, mostly from input provided by the involved persons themselves; no person-related data beyond the minimum required for processing authenticated access to the OePG website is collected or processed by its websites. The OePG does not use strategies like tracking or profiling of the activities of its members or of other visitors of its websites.

This data protection declaration comprises the handling of data on the central administration system of the OePG, on its website (https://www.oepg.at), the website of its section "*Young Minds*" (https://www.oepg-ym.at or http://www.oepg-students.at), and data kept outside these systems, partly in non-electronic form.

The OePG is controller as well as processor in the sense of the General Data Protection Regulation (GDPR) of the EU. The documents required by the GDPR, in particular, records of processing activities, have been prepared. We will detail below the information of immediate interest for the members of the OePG, and relevant for the users and the contents of its websites.

2. Member Data

2.1. Collected and Stored Data

- Member number
- Category of membership
- Dates of beginning and, if applicable, end of membership
- Access data for pages of the websites listed above that are restricted to OePG members or hold individual information on a member, and to the individual PayPal® payment page for the member
- Name, gender and, if applicable, titles
- Date of birth (year of birth is sufficient)
- Postal addresses (optionally two addresses, e.g., for special invoices)
- E-mail addresses (up to three addresses)
- Phone and fax numbers (up to three numbers each)
- Personal homepages (up to three addresses)
- Affiliations to divisions or sections of the OePG (optional)
- Memberships of other societies (optional)
- Preferences on transmission of information (electronically or in hardcopy) or delivery of journals, in particular, of "*Europhysics News*"

- Subscription to the "*Physik Journal*" (optional)
- Communication language (German or English)
- Administrative notes of the member and the OePG administration
- Membership account; we register invoices, payments, credit and debit notes for membership fees, donations, and in the case of a subscription to the "*Physik Journal*", charges for each single issue of the journal at the time this issue is ordered

2.2. Use of the Data

On principle, the member data listed above are solely used by the central administration of the OePG for fulfilling the Society's purpose (e.g. for mailings) and for administrative tasks such as creating membership fee invoices and processing payments of membership fees and donations. A strongly reduced subset of this data serves for authentication purposes on the websites of the OePG (https://www.oepg.at) and its section „*Young Minds*" (https://www.oepg-ym.at or http://www.oepg-students.at) to allow individual access of members to information not commonly accessible.

2.3. Viewing Rights

Upon registration with the OePG, each member has received credentials which allow inspection and modification of her or his own data and of her or his membership account on the website of the OePG (https://www.oepg.at). Members are encouraged to replace the random default password they received from the OePG with a password of their own choice.

2.4. Disclosure of Data

Personal data of members are nowhere publicly visible, and each member has exclusive access to her or his own data only. The OePG administration sends mails individually to each member; it is therefore not possible to extract names or mail addresses of other members from such mailings. However, the OePG must pass on member data to third persons (to the minimum extent required for the particular purpose) in the following cases:

- Contact data of members of divisions or sections of the OePG: The names and postal and/or e-mail addresses of members who have declared their association with a particular division or section of the OePG may be passed on to the chair or deputy chair of this division or section if required. The recipients of the member contact data are obliged, though, to treat the data confidentially and under no circumstances to pass them on to third persons. This implies that e-mails be sent as blind carbon copies, with no visible list of mail addresses. Furthermore, the persons who have received member data must not use this data for any purpose not directly connected to the work of their division or section, and they must not use them anymore and delete them reliably upon termination of their period as chairs or deputy chairs. (Alternatively, the central administration of the OePG can create individual mailings to any group of OePG members.)
- Orders of the "*Physik Journal*": The "*Physik Journal*" is shipped directly to its subscribers by the publishing house (*Wiley*) which issues it. The OePG must provide a list of the current subscribers for each issue, which does not contain information beyond member numbers, names and delivery addresses.
- Payments of membership fees or donations with PayPal®: The PayPal® payment page on the OePG website invokes a web page provided by PayPal®. The only information passed on to the PayPal® page is the amount of the payment, though.

- Matching of membership data with "friendly" societies: There are mutual agreements of the OePG with foreign societies, in particular, the German and Swiss Physical Societies, which grant members of one of these societies certain reductions of their membership fees with the other societies. The involved societies have to periodically check the claims asserted by their members by exchanging lists of their members who claim a membership of a "friendly" society. This entails exchange of the data required for the identification of these persons, i.e. their names and possibly addresses. In the normal case where a person is indeed member of several societies, no data is actually passed on since the information is already available at the society that receives the data for matching.
- Members of the "extended board" of the OePG: The OePG publishes the names and certain contact data of the members of its "extended board", i.e., president, vice president, manager, members of the official board, chairs and deputy chairs of divisions and sections of the OePG, and its auditors. The data published are derived partly from the member data listed above; however, it is possible to define data especially for this purpose. The following rules apply:
  - For president, vice president and manager, the OePG displays, if possible, a complete contact address, including phone and fax numbers and e-mail addresses. Optionally, a picture may be included. For all other persons, the OePG displays postal (if applicable) and e-mail addresses, and optionally a picture.
  - It is possible to configure all information except the names independently from the membership data proper. The postal address may be suppressed if desired, and the OePG can provide upon request special e-mail addresses for display on the website.

2.5. Right of Access by the Data Subject

Each member can inspect her or his own data and documents on her or his membership on pages on the website of the OePG exclusively available to the member via an authenticated access. All information on data protection, amount and use of personal data of members is detailed in this document.

2.6. Right to Rectification

Each member can correct her or his own data on a page on the website of the OePG exclusively available to the member via an authenticated access. Accounting errors affecting payments of membership fees or donations can be corrected at short notice, within 30 days maximum, once a suitable proof of payment has been submitted.

2.7. Right to Erasure, Right to Restriction of Processing, Right to Object

The data items listed above and their use by the OePG (see section 2.2) is indispensable for the whole duration of a membership. The above rights are therefore only available after the termination of a membership.

2.8. Right to Data Portability

The data of a member and a summary of her or his membership account may be provided in one of several common data formats if required.

2.9. Duration of Data Storage

As detailed in section 2.7, the OePG must keep the data of its members at least up to the end of a membership. For technical reasons, it is not possible to completely delete the database records related to a membership; however, the OePG obfuscates the data in a way that prevents an identification of the member based on data avail-

able at the OePG. The OePG carries out this obfuscation three months after the termination of a membership if the member's membership account is balanced; otherwise, the member data must be kept for three years after the end of a membership until the legal limitation period is expired. (The delay of a minimum of three months is required to allow members whose membership has been terminated by the OePG to return to the OePG when the reason for the termination of their membership has ceased.)

2.10. Miscellaneous

On principle, the OePG does no more dispatch mails with personal data of one or more members. Documents or lists containing individual-related data are kept on the administration system, well protected against unauthorized access. They may be retrieved over a secure (HTTPS) connection if required.

The website and administration server of the OePG generate mails to members upon certain actions, e.g., certain changes of membership data or certain accounting transactions. Under certain circumstances, copies of these mails may also be sent to administrative staff of the OePG. These mails do not contain individual-related data. Documents created in the course of these actions (e.g., member data sheets, proofs of membership or payment, account statements) are stored within the administration system and may be downloaded by the member over a secure connection after an authenticated login at the OePG website (https://www.oepg.at).

The OePG may create lists of members (with postal or e-mail addresses) in the following cases:

- Order lists for the publisher of the "*Physik Journal*": Access to the OePG administration system has been granted to a person nominated by the publishing house. This person has only the right to download order lists over a secure connection. The OePG has to archive these order lists for the full duration of the legal limitation period to be able to respond to possible claims of a subscriber, i.e., for at least three years after their generation.
- List of the recipients of mails sent to a group of or all members: These lists are needed to check who has received which mailing. The OePG has to archive these lists for the full duration of the legal limitation period to be able to respond to possible claims of a member, i.e., for at least three years after their generation.
- Control files for hardcopy mailings: These files are needed to check who has received which mailing. The OePG has to archive these files for the full duration of the legal limitation period to be able to respond to possible claims of a member, i.e., for at least three years after their generation.
- Log files of the administration system: These log files are created during daily data runs. They contain names and member numbers and, possibly, records of actions performed for the particular member. The OePG has to archive these files for the full duration of the legal limitation period to be able to respond to possible claims of a member, i.e., for at least three years after their generation.
- Correspondence: The OePG must archive letters and mails from and to members for the full duration of the legal limitation period to be able to respond to possible claims of a member, i.e., for at least three years after their generation.

Unless legal or archive considerations speak against deleting data, the OePG will delete the documents listed above after the mentioned three years period.

3. Physics Research Groups in Austria

3.1. Collected and Stored Data

- Name, gender and title of the head of the research group
- Postal address of the head of the research group
- E-mail addresses (optionally up to three addresses) of the head of the research group
- Up to three addresses of websites of the research group
- Access credentials that allow editing of the information on the research group at the OePG website
- Affiliation of the research group to research areas and to fields of work according to the Austrian System of Science Areas

3.2. Use of the Data

Display on the website of the OePG (https://www.oepg.at).

3.3. Viewing Rights

The information items listed above are published on the website of the OePG (https://www.oepg.at). They can be freely inspected and modified by the head of the research group via an authenticated access to the website.

3.4. Disclosure of Data

The information on research groups is intended for public display on the OePG website (https://www.oepg.at).

3.5. Right of Access by the Data Subject

Each head of a research group can inspect the data pertaining to her or his group on the website of the OePG. All information on data protection, amount and use of the data is detailed in this document.

3.6. Right to Rectification

Each head of a research group can correct the data pertaining to her or his group, if required, via an authenticated access to the website of the OePG.

3.7. Right to Erasure, Right to Restriction of Processing, Right to Object

Research groups can upon request be hidden or completely deleted.

3.8. Right to Data Portability

There are no routine provisions for the export of data of a research group. If necessary, the OePG can provide means to export research group data in a standardized format.

3.9. Duration of Data Storage

The data of research groups are needed for the display of the information on these groups on the OePG website. Data storage is therefore needed for the entire period during which this display is needed.

4. Registration to Events of the OePG

The administration system and the website of the OePG contain functions that permit the registration of participants for events hosted by the OePG itself or one of its divisions or sections. These registration functions are only activated when needed.

4.1. Collected and Stored Data

- Selected event, category of participant and possible additional offer pertaining to the event
- Gender, name and titles, if applicable, of the participant
- Postal address of the participant (optional)
- E-mail address of the participant
- OePG member number of the participant if applicable
- Communication language (German or English)
- Password defined by the participant and stored in encrypted form to permit further inspection and modification of the registration data on the OePG website (https://www.oepg.at)
- Invoice for a participant's fee, and information on its payment

4.2. Use of the Data

Administration of registrations to events hosted by the OePG or one of its divisions or sections, and of payments of registration fees.

4.3. Viewing Rights

Upon registration, each participant receives individual information that allows, in conjunction with the self-defined password, inspection and modification of her or his registration data at the OePG website (https://www.oepg.at).

4.4. Disclosure of Data

Access to registration data is only permitted for a specially nominated person who administrates the particular event. Participants may inspect and edit strictly their own data, no data of anybody else. The organizers of an event may create a list of participants; they are, however, responsible for a correct adherence to data protection regulations.

4.5. Right of Access by the Data Subject

Each participant may inspect her or his own registration data via an authenticated access to the OePG website. All information on data protection, amount and use of the data is detailed in this document.

4.6. Right to Rectification

Each participant may correct her or his own registration data via an authenticated access to the OePG website.

4.7. Right to Erasure, Right to Restriction of Processing, Right to Object

After the cancellation of a registration or the end of the event, the data of participants are erased or obfuscated to prevent their identification.

4.8. Right to Data Portability

There is no routine procedure for the export of records of single participants; however, it is possible to export such data in a standard format.

4.9. Duration of Data Storage

The data of participants are required for processing the event. They must therefore be kept until at least the end of the event. In general, the OePG obfuscates them one month after the end of the event in a way that prevents identification of individual persons based on the information available at the OePG. Exceptions to this rule are participants with an open balance, even after they cancelled their registration; in this case, their data must be kept for the full three year legal limitation period. The OePG obfuscates their record after three years.

5. Administrators

Administrators are in charge of the contents of the administration system and the website of the OePG (https://www.oepg.at). There are separate administrators for the website of the section "*Young Minds*" (https://www.oepg-ym.at or http://www.oepg-students.at) who have rights only within that website. The information given here applies to them analogously, though.

5.1. Collected and Stored Data

- Login name
- Password for the administration system or directory
- Full name
- E-mail address
- Authorizations: Each administrator can individually receive the right to access any single function of the administration system. It is possible, for example, to grant an administrator access to certain contents of the website but not to the data of members.

5.2. Use of the Data

Administration of authorizations within the OePG administration system or the OePG website; or of authorizations within the administration system of the website of the section "*Young Minds*", respectively.

5.3. Viewing Rights

All administrators have, as a minimum, the right to change their own password. Depending on the area of responsibility and the authorizations granted to an administrator, she or he may be permitted to change her or his own data.

5.4. Disclosure of Data

Administrators who have received the right to edit accounts of other administrators may inspect the account data of administrators belonging to the same class of administrators (common or master administrators), and they may pass on their own rights to other administrators. This guarantees that new administrators under no circumstances can have rights exceeding those of the person who created their accounts. Neither own nor foreign passwords may be inspected, though.

5.5. Right of Access by the Data Subject

Each administrator may inspect her or his own data in the OePG administration system. All information on data protection, amount and use of the data is detailed in this document.

5.6. Right to Rectification

Depending on the authorization granted, each administrator may either correct herself / himself her / his own data if necessary, or alternatively ask another administrator for correction.

5.7. Right to Erasure, Right to Restriction of Processing, Right to Object

No more required data of inactive administrators and their accounts may be erased. The data of active administrators are still required; however, it is possible to make restrictions to their authorizations.

5.8. Right to Data Portability

There is no routine procedure for the export of records of single administrators; however, it is possible to export such data in a standard format.

5.9. Duration of Data Storage

Data of administrators are required for the full period of their activities. They may be deleted afterwards.

6. Various contents of the websites of the OePG and its section "*Young Minds*"

These websites publish information that either the OePG receives from third persons with the intent of publication (e.g., press releases), or which has been generated by members of the OePG. In the latter case, it lies within the responsibility of the administrator who uploads these contents to make sure that their publication does not infringe the rights or interest of other persons. This rule applies to textual contents as well as to images. In case the OePG receives contents from external sources who are subject to the General Data Protection Regulation (GDPR) of the EU, the OePG can reasonably assume that all personal rights possibly involved have been properly protected. No web publication is permitted in case of doubt.

The two websites feature areas that are only accessible after a previous login at the website; this allows publishing certain contents to members only. Optionally, uploaded documents may be, in addition, encrypted. They are decrypted on the fly for properly authenticated users.

6.1. Collected and Stored Data

Various data; person-related only to a small degree.

6.2. Use of the Data

Publication on the websites of the OePG (https://www.oepg.at) and/or of its section "*Young Minds*" (https://www.oepg-ym.at or http://www.oepg-students.at).

6.3. Viewing Rights

All data in this category are displayed on the website in their entirety. There are no data that are not visible over the website.

6.4. Disclosure of Data

The contents are intended for publication on one of the websites listed above. Access to them may be restricted to OePG members properly logged in to the particular website.

6.5. Right of Access by the Data Subject

All information on data protection, amount and use of the data is detailed in this document.

6.6. Right to Rectification

In accordance with the General Data Protection Regulation (GDPR), the OePG will comply with any reasonable request to rectification of faulty data or data conflicting with the interest of persons involved as quickly as possible, within a maximum of 30 days.

6.7. Right to Erasure, Right to Restriction of Processing, Right to Object

In accordance with the General Data Protection Regulation (GDPR), the OePG will comply with any reasonable request to erasure by persons affected by contents on its websites within a maximum of 30 days. The OePG does not perform any further processing of contents published on its websites; the rights to restriction of processing and to object are therefore implicitly met.

6.8. Right to Data Portability

Data on the websites of the OePG are available for free use.

6.9. Duration of Data Storage

Unless contents have been deleted due to an explicit request they remain indefinitely active and visible, at least in the archive areas of the websites.

7. Accounting Data of the OePG

The accounting data of the OePG, i.e., information and documents on revenues and expenses of the OePG and its divisions and sections may contain person related data and are therefore also subject to a treatment in accordance with the General Data Protection Regulation (GDPR). For example, person-related data may be involved in the following cases (the OePG does not claim completeness of the list below):

- Payments of membership fees or donations
- Bills for services rendered and expense allowances
- Travel expenses and other expenses
- Reimbursements of costs incurred with purchases on behalf of the OePG

7.1. Use of the Data

Preparation of the legally required accounting of revenues and expenses of the OePG; budget planning.

7.2. Viewing Rights

All accounting information is to be treated confidential. Persons who do not belong to the group of persons defined in section 7.3 may, as a maximum, have the right to view documents related to themselves.

7.3. Disclosure of Data

Within the OePG, only the following persons have the right to inspect accounting documents:

- Persons who are responsible for partial accounting, within the scope of their own accounting
- Members of the board of the OePG
- Internal auditors of the OePG

Accounting Documents may be passed on to

- External auditors
- Tax consultants of the OePG

According to the statutes of the OePG and legal requirements, an anonymized version of the OePG's accounting that does no more allow the identification of single transactions and the persons involved in them must be prepared and presented to the members during the general assembly.

Any further disclosure of accounting data to individuals within or outside the OePG is not permitted.

7.4. Right of Access by the Data Subject

All information on data protection, amount and use of the data is detailed in this document.

7.5. Right to Rectification

The right to rectification of erroneous bookings (e.g., of membership fee payments) or money transfers (e.g. in the course of reimbursements) is granted, provided a proper proof is available. Within the limits of technical and legal possibilities, the OePG will rectify such mistakes within a maximum of 30 days.

7.6. Right to Erasure, Right to Restriction of Processing, Right to Object

The OePG will grant those rights if they are applicable to the case in mind and do not contradict other conditions, e.g., legal issues.

7.7. Right to Data Portability

In consideration of sections 7.1 and 7.3, data available in electronic form may be provided for export in a standard format.

7.8. Duration of Data Storage

Accounting records have to be kept for at least the period of seven calendar years required by finance law.

8. Miscellaneous Data

In the course of its operations, the OePG may have to collect additional information that may contain person related data. For example, the OePG or its branch organizations award prices, which must be applied for. The applications must be backed by a suitable proof of the qualifications of the candidates, and they usually are submitted to an external peer review. All documents received in the course of the applications and reviews are to be deleted when one year's prices have been awarded and the price money has been paid. The names of the awardees and the reasons for award-

ing a price to them must, however, be indefinitely stored for archival reasons; they are also published on the website of the OePG.

9. Measures for Ensuring Data Security and Data Integrity

The data electronically stored in the administration system of the OePG reside on a server at the Technical University (TU) Vienna which is operated and professionally maintained according to the state of the art by staff of the IT department of the TU Vienna (TU-IT). Access to this server is restricted by various measures. The design of the system guarantees that access to its database and thus to person-related data is only possible from within the administration system. Only a small number of administrators (see section 5) may access the administration system after a preceding login with user name and password. All logins are logged. There are, as usual, special service interfaces for the server itself and the database; access to these interfaces requires a strict login and is limited to a very small number of internet addresses. A special maintenance tool periodically checks the software installed on the administration system for unexpected changes; this allows detecting and fighting attempts to intrude into the system at a very early stage.

The websites of the OePG (https://www.oepg.at) and of its section "*Young Minds*" (https://www.oepg-ym.at or http://www.oepg-students.at) are hosted at a commercial provider. Since these websites are more exposed than the administration system they routinely hold member data only to the extent absolutely necessary for controlling access to protected information (i.e., name, member number and one-way encrypted password). A complete member record is only loaded on the OePG website when a correctly authenticated member enters the page for editing his or her membership data. For a short period of time, the complete member data record is held in the database of the website when the editing page has been submitted; however, administrators responsible for member data are automatically notified of any such change, and after checking and, if applicable, accepting or rejecting the changes and copying them to the base member data on the administration system the record on the website is shortened to its previous extent. Since this normally happens within a few hours after a change to a member's data the danger is small that member data may get into the wrong hands if the website becomes compromised. A special maintenance tool periodically checks the software installed on the websites for unexpected changes; this allows detecting and fighting attempts to intrude into the system at a very early stage. Information reserved to OePG members can be placed on pages specially reserved for this purpose which are only accessible after a successful login of a member at the website. In addition, uploaded files may be encrypted; they are automatically decrypted for properly authenticated members only.

The transmission of data between the administration system and the above websites runs in encrypted form over an SSL-secured connection. The administration system enforces generally the use of Secure HTTP (HTTPS); Standard HTTP-based accesses to the website of the OePG (https://www.oepg.at) and to the new website of its section "*Young Minds*" (https://www.oepg-ym.at) are automatically converted to Secure HTTP wherever possible (not for very old browsers and/or operating systems). This guarantees a login to the website and a retrieval of (personal) documents over a secure connection. (The OePG keeps the old website of its section "*Young Minds*", (http://www.oepg-students.at), which is only available via standard HTTP, for a limited period of time to keep the results stored in search machines valid. However, all accesses to the old website are immediately redirected to the new "*Young Minds*" website.)

Unless person-related data are intended anyway for a display on a website (as in the case of the physics research groups), they are no more transmitted by regular e-mail. The OePG has installed a special page on its website (https://www.oepg.at) where members can download all documents related to their membership via a se-

cure connection after a login to the website. Each member has, of course, only access to her or his own documents. These documents are, by the way, not stored on the website but retrieved, when requested, directly from the administration system over a secure connection. They may therefore in no way be compromised in the case of an attack against the OePG website.

The OePG website (https://www.oepg.at) uses payment functions provided by PayPal®. PayPal® is known to impose very high standards to the SSL encryption used for invoking its services. Making sure that PayPal® transactions are properly possible simultaneously ensures that the server on which the OePG website resides uses state of the art security standards.

User-defined passwords are stored in the database as a one-way encrypted hash. Except by using brute force methods, it is not possible to reconstruct a user-defined password. In contrast, the default passwords created at the registration of new members are held in the database (on the administration system only) to allow passing them on to the members if forgotten; members are encouraged, though, to create themselves user-defined passwords that are not known to anybody else.

The developer of the software tests the systems of the OePG under his control periodically for the appropriateness and accuracy of the various security measures used. This resulted, for example, in the use of improved algorithms for the storage of (user-defined) passwords which strongly increase the effort needed for cracking them. However, even in case the websites of the OePG (https://www.oepg.at) or its section "*Young Minds*" (https://www.oepg-ym.at or http://www.oepg-students.at) were compromised, the data obtainable from them would be hardly useful for third persons.

Occasionally, the security checks carried out by the OePG itself are augmented by having "high-level" hackers test, in particular, the websites. There are organizations on the web, e.g. *OpenBugBounty.org*, where volunteer security specialists apply methods used by criminal hackers, however without creating damage. Their input is particularly valuable because they point out possible problem areas we were not aware of before. Although hardly any of the vulnerabilities pointed out to date had really been dangerous we have fixed them very thoroughly.

The contents of the database and the software of the administration system are secured in periodic backups. Backups are performed cyclically, i.e., the newest backups overwrite the oldest ones. Old backups may possibly be of interest for forensic reasons (i.e., at which point in time some unwanted changes have happened); if there is the need to restore data from a backup (which happens extremely rarely), the newest suitable backups are used. This strongly reduces the danger to revive data that have meanwhile be deleted or obfuscated: Manual deletions are very rare; they may simply be repeated. Records which have been deleted or obfuscated because they were expired are simply once more deleted or obfuscated during the next data run.

The accounting records for membership accounts contain a hash value, which immediately allows detecting and reporting any manipulation carried out with the data.

Data available electronically that are not routinely kept on the administration system are stored according to the state of the art on the computers of those persons within the OePG who are responsible for processing them. They are deleted in consideration of possible legal or archival conditions if they are person-related and there is no need to keep them anymore.

The OePG stores hardcopy documents in locked rooms. They are deleted in consideration of possible legal or archival conditions if they are person-related and there is no need to keep them anymore.