Scope of processed personal data

- First name
- Last name
- Private e-mail address

Information on the main content of joint arrangements of the Joint Controllers along with information on the processing of personal data.

Information about the processing of your personal data

According to art. 13 and art. 26 of Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of data personal data and on the free movement of such data and the repeal of Directive 95/46/EC, hereinafter referred to as "GDPR", we inform you that we jointly process your personal data and inform you about the main content of joint arrangements of the Joint Controllers.

Details about this collaboration

I. Co-Joint Controller of personal data

Please be advised that the Co-Joint Controllers of your personal data are:

a) SWPS University – Data Protection Officer: iod@swps.edu.pl
b) Copenhagen Business School – Data Protection Officer: dpo@cbs.dk
c) Bruegel – Data Protection Officer: siobhan.mulvey@bruegel.org
d) Merics – Data Protection Officer: steffen.buchholz@merics.de
e) SciencePo – Data Protection Officer: nawal.lamrini@sciencespo.fr
f) Asia Centre – Data Protection Officer: jb.monnier@asiacentre.eu

II. Data Protection Inspectors

The Controllers can be contacted in writing at the address of the registered office that has appointed a Data Protection Officer. You can contact the Data Protection Officer of the Controller I regarding the protection of your data and the exercise of your rights by email: iod@swps.edu.pl

You can also directly contact any Controllers in application of (Article 6(1)(a) of the GDPR).

III. Data recipients

Authorized employees and associates of all Controllers will have access to your data, and the recipients of the data may be entities cooperating as part of the implementation of the DWARC project as well as entities providing the Controller(s) with services that require providing personal data to set up an account in the IT system (especially if the Event will take place in remote mode).

In the event of necessity, your personal data may also be made available only to entities authorized to receive your data on the basis of applicable law, which, within the meaning of the GDPR, will not be recipients of data, but require providing data to perform their tasks specified in the regulations.

IV. Data transfer to third countries

With the exception of storage in the IT cloud and the use of data to ensure the possibility of using the university account in the Google Workspace for Education system, we do not transfer your data outside the European Economic Area.

V. Period of data storage

Your data obtained for the purpose of carrying out the DWARC project will be stored for the project duration and deleted afterwards. The project will end 31 October 2025. Due to the possibility of publishing information about Participants allowed by the Event Organizers and their images as well as recorded audio and video recordings, the withdrawal of consent to such publication will not affect the processing carried out before the withdrawal of consent. If you withdraw your consent, the documents provided on the basis of your consent will be anonymized if one of the conditions set out in article 17 of the GDPR is met, including the data are no longer necessary for the purposes for which they were collected.

Your rights

You are entitled to:

a) the right to access your personal data - obtain confirmation from the Joint Controllers whether your personal data is being processed, and if this is the case, obtaining access to them and providing you with information in the scope indicated in art. 15 GDPR;

b) the right to rectify your personal data - request the Joint Controllers to immediately rectify incorrect personal data and supplement incomplete personal data in accordance with art. 16 GDPR;

c) the right to delete your personal data - request the Joint Controllers to immediately delete personal data if one of the conditions specified in article 17 of the GDPR is met, including the data are no longer necessary for the purposes for which they were collected. The right to delete data may be limited due to the Controller's obligations under applicable law;

d) the right to limit the processing of your personal data in the cases indicated in art. 18 GDPR, e.g. contesting the accuracy of personal data;

e) the right to object to the processing of your personal data in the cases specified in art. 21 GDPR;

f) the right to lodge a complaint with the data protection supervisory authority personal data in accordance with art. 77 GDPR;

In order to exercise the above-mentioned rights, a request should be sent to any of the Joint Controllers. Please remember that before exercising your rights, the Joint Controllers will have to make sure that you have the above right, i.e. identify you accordingly.

Providing data

Providing your data is mandatory to receive emails from the selected scope. Failure to provide your personal data will prevent you from receiving anyt newsletter.

In connection with the processing of your personal data, we also inform you that:

a) The Joint Controllers declare that they process your personal data in accordance with the rules regarding the processing of personal data set out in art. 5 GDPR;

b) Joint controllers keep the documentation on co-controlling for the purposes of meeting the accountability requirement;

c) Joint controllers undertake to limit access to your personal data only to persons whose access to personal data is necessary for the implementation of the above-mentioned purposes. In addition, all Controllers ensure that only authorized persons are allowed to process personal data, and that persons authorized to process personal data have been obliged to keep personal data secret, and that these persons have previously been trained in the principles and regulations on data protection. personal data;
d) The Joint Controllers ensure an appropriate level of personal data security including:

- ability to ensure confidentiality, integrity, availability and resilience at all times personal data processing systems and services;
- the ability to quickly restore the availability and access to personal data in the event of a physical or technical incident.