

Privacy Statement¹ – Social Media Assurance Service (SMAS)

1. Introduction

The Single Resolution Board (SRB) processes your personal data in accordance with the Regulation (EU) [2018/1725](#) (EUDPR). The privacy statement explains the reasons for processing your personal data, the way the SRB collects, handles and ensures protection of all personal data. It also specifies the contact details of the responsible SRB unit where you may exercise your rights, the SRB Data Protection Officer and the European Data Protection Supervisor (EDPS)

2. Who is responsible for processing your personal data?

The SRB is the controller for processing the personal data. The SRB's ICT Team is responsible for the processing. The processing operation will be carried out with the support of an external third party, the CERT-EU. CERT-EU processes the personal data on behalf of the SRB. The SRB has in place a Service Level Agreement (SLA) with CERT-EU in this context. For further details, you may also read the CERT-EU's privacy statement [here](#).

3. Why do we process your personal data?

SMAS analyses profiles across social media channels² (on the basis of specific keywords defined by the SRB) to identify accounts pretending to be associated with the SRB's brand, the SRB Chair and/or Vice-Chair. SMAS is an artificial intelligence based platform, which can rapidly identify cyber and physical risks across social media channels.

4. What are the legal bases for processing your personal data?

Article 5(1)(a) in conjunction with Recital 22 of EUDPR and the SRB Founding Regulation ("SRMR", Regulation (EU) No 806/2014) serve as legal bases for this processing. This processing of personal data is necessary to ensure the proper management and functioning of the SRB (e.g. protect the SRB from impersonation: fake account on social media).

5. What categories of personal data are processed?

SMAS may collect information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular person.

SMAS may collect the following categories of personal information from a particular person within the last twelve (12) months:

- Identifiers
- Commercial information

¹ Last update 27/02/2023

² Twitter, Facebook, LinkedIn, Google+, YouTube, and Instagram.

The category “identifiers” gathers real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, or other similar identifiers.

The personal data are used by the SMAS to identify accounts pretending to be associated with the SRB’s brand, SRB’s Chair and/or SRB’s Vice-Chair and their post content

6. Who has access to your personal data?

Employees of SRB ICT Security team and the CERT-EU has access to those “key words” and may access the results of the process on a strict need-to-know basis.

7. In which third country personal data could be transferred?

Personal data is not transferred to third countries. The “key word” information are stored in servers located in European Economic Area and managed by Zerofox and Cert-EU. Zerofox has a [certification](#) on value and importance.

8. How long will the SRB keep your personal data?

The results of the process are stored for a maximum of 2 years and then deleted.

9. What are your data protection rights?

You have the right to access your personal data and correct any data that is inaccurate or incomplete. You have also (with some limitations) the rights to delete your personal data, to restrict or to object the processing of your personal data in line with the Regulation (EU) 2018/1725.

10. Who can you contact in case of queries or requests?

You can exercise your rights by contacting the ICT Unit Local Information Security Officer of SRB (IT-SEC@srb.europa.eu). The SRB’s Data Protection Officer at SRB-DPO@srb.europa.eu answers all queries relating to personal data protection.

11. Addressing the European Data Protection Supervisor

If you consider that your rights under Regulation (EU) 2018/1725 have been violated as a result of the processing of your personal data, you have the right to lodge a complaint with the [European Data Protection Supervisor](#) at any time.