ePrivacyseal

ePrivacy Vendor Compliance Seal

Criteria Catalogue

version 1.0

7th July 2022

The ePrivacy Vendor Compliance Seal certifies for the respective applicant that its product or service is in line with the detailed criteria in the following criteria catalogue based on the requirements of the IAB EU TCF Transparency and Consent Framework and the respective data protection requirements from GDPR.

A. Legal basis

1. The Vendor has defined its data protection role (controller, processor, joint controller) for all processing activities.

   applicable rules: (preliminary question)

2. The Vendor shall base its processing activities on consents collected via the TCF and/or legitimate interest secured via the TCF 2.0, with all processing activities covered by the registered Purposes, Special Purposes, Features and Special Features.

   applicable regulations: art. 6(1) GDPR, § 25 TTDSG, TCF Policies 10.2., 10.5., 16.3

3. The Vendor will not store or access data on User Equipment and will not process any further data without the User's prior verifiable consent (unless there is a legal exception to the consent requirement) or legitimate interest and the absence of an objection by the User.

   applicable regulations: art. 6(1) GDPR, § 25 TTDSG, TCF Policies 16.1., 16.2., 16.8., 16.9.

4. If the Vendor is a processor, it has entered into a proper contract processing agreement with the controller; if it is a joint controller, it has entered into a proper corresponding agreement with the controller.

   applicable provisions: art. 26, 28 GDPR

5. The Vendor will only process automatically sent device properties for identification purposes without a corresponding indication in the Global Vendor List in order to use them for security purposes, fraud prevention and error detection and if
   – the Vendor has carried out a data protection impact assessment,
   – the Vendor limits data processing to what is necessary,
   – the Vendor complies with reasonable retention periods, and
   – the data collected in this context is not used for any other purpose.

   applicable regulations: TCF Policies 16.11.

6. The Vendor shall not process any data for a Special Feature without the User's prior, appropriate and verifiable consent by means of a corresponding signal.

   applicable regulations: TCF Policies 16.12.

7. The Vendor will only process Precise Geodata without the User's consent if it is either immediately rendered imprecise and the Precise Geodata is not processed for any other purpose, or to use it for security, anti-fraud and error detection purposes and if
   – the Vendor has carried out a data protection impact assessment,
   – the Vendor limits the data processing to what is necessary,
   – the Vendor complies with reasonable retention periods, and
   – the data collected in this context is not used for any other purpose.

   applicable regulations: TCF Policies 16.13.

8. The Vendor collects device characteristics for identification purposes without the User's consent only for security, anti-fraud and error detection purposes and if
   – the Vendor has conducted a data protection impact assessment,
   – the Vendor limits data processing to what is necessary,
   – the Vendor complies with reasonable retention periods, and
   – the data collected in this context is not used for any other purpose.

   applicable regulations: TCF Policies 16.14.

9. The Vendor shall only transfer personal data to another Vendor if the latter has a legal basis for their processing by means of a corresponding signal.

   applicable regulations: TCF Policies 16.15.

10. The Vendor shall only transfer personal data to a third party outside TCF 2.0 if the third party has a legal basis for processing it.

    applicable regulations: TCF Policies 16.16.

B. Transparency and data subject rights

11. The Vendor has a full, legally compliant, easily accessible, public privacy policy on its website.

    applicable regulations: art. 12, 13, 14 GDPR, TCF Policies 10.3.

12. The Vendor has publicly confirmed its participation in TCF 2.0 and its compliance with the policies by stating the Vendor ID, for example in a privacy policy.

    applicable regulations: TCF Policies 11.2.

13. The Vendor has a process for dealing with data subject rights.

    applicable provisions: art. 15 et seqq. GDPR

C. Data security

14. The Vendor has implemented sufficient technical and organisational measures for data security.

    applicable provisions: art. 25, 32 GDPR

D. Documentation

15. The Vendor shall keep a register of its processing activities.

    applicable provisions: art. 30 GDPR

16. The Vendor has appointed a data protection officer and registered them with the supervisory authority.

    applicable provisions: art. 37 GDPR

17. The Vendor has carried out a threshold analysis and, if positive, a data protection impact assessment.

    applicable provisions: art. 35 GDPR

E. International data transfers

18. If an (onward) transfer (including direct collection and (potential) access to) unencrypted personal data to/from a non–EEA country without an adequacy decision, such as the United States, takes place on the basis of the standard contractual clauses, (1) no law applies to any of the data recipients that obliges the recipient to hand over the data or the key without adequate legal protection for the data subjects OR (2) additional technical and

organizational measures are taken (and, if applicable, contractually agreed) to ensure an adequate level of data protection AND a transfer impact assessment has been carried out.

applicable provisions: art. 46 para. 2 lit. c GDPR

F. Handling TCF signals

18. The Vendor shall comply with the Specifications, in particular it shall record or pass on Signals in the specified technical formats.

    applicable regulations: TCF Policies 12.1.

19. When processing data according to the TCF 2.0, the Vendor only processes signals from CMPs that comply with the Policies, in particular that are registered with IAB Europe and have publicly confirmed compliance.

    applicable regulations: TCF Policies 13.1.

20. The Vendor processes data according to the signals received from the CMPs. The Vendor only processes signals in real time and not stored signals.

    applicable regulations: TCF Policies 13.3.

21. Signals that the Vendor cannot process are interpreted as a lack of authority to process data.

    applicable regulations: TCF Policies 13.4.

22. If the signal is not sufficient, the Vendor does not process any data.

    applicable regulations: TCF Policies 13.5.

23. The Vendor does not create any signals itself, but only processes and transmits unchanged signals of a CMP.

    applicable regulations: TCF Policies 13.6.

24. The Vendor receives signals according to the Specifications and using the API.

    applicable regulations: TCF Policies 13.7.

25. When processing data in accordance with TCF 2.0, the Vendor shall only process data from Publishers who comply with the Policies, in particular who have publicly confirmed their compliance.

    applicable regulations: TCF Policies 14.1.

26. The Vendor observes contractual obligations towards the Publishers, even if a signal may permit further data processing.

applicable regulations: TCF Policies 14.3.

27. The data processing software used by the Vendor (including scripts and tags) is configured to comply with the Specifications and the Policies, in particular that no data is processed without a verifiable legal basis by an appropriate signal and no data is stored or accessed on User Equipment without verifiable prior consent by an appropriate signal, unless there is an exception to the consent requirement.

    applicable regulations: TCF Policies 14.4.

28. The Vendor shall update data processing software (including scripts and tags) provided by other Vendors as necessary to comply with the Specifications and Policies.

    applicable regulations: TCF Policies 14.5.

29. If necessary, the Vendor forwards signals from a CMP or another Vendor to other Vendors.

    applicable regulations: TCF Policies 14.6.

30. The Vendor shall keep records of consents where required by the Policies and Specifications.

    applicable regulations: art. 7(1) GDPR, TCF Policies 15.1.

31. The Vendor shall keep records of user IDs, timestamps and signals received for the duration of the data processing.

    applicable regulations: art. 7(1) GDPR, TCF Policies 15.2.

G. TCF registration and procedure

32. The Vendor is registered as a Vendor with IAB Europe in accordance with TCF 2.0.

    applicable regulations: TCF Policies 10.1.

33. The Vendor has disclosed its legal structure and its ability to maintain its services and compliance with the Policies to IAB Europe.

    applicable regulations: TCF Policies 10.4.

34. The Vendor has provided complete and accurate information when registering with IAB Europe, in particular on the Purposes, Special Purposes, Features and Special Features of its processing activities, the relevant legal basis, and the storage of or access to data on user devices. These details are recorded in the Global Vendor List.

    applicable regulations: TCF Policies 10.2., 10.5., 16.4.–16.7., 16.10.

35. The Vendor shall indicate on the Global Vendor List whether it wishes to obtain consents for storage of or access to data on user devices.

    applicable regulations: TCF Policies 16.2.

36. The Vendor shall indicate on the Global Vendor List the maximum storage period of the data stored on user devices and whether the storage period can be extended.

    applicable regulations: TCF Policies 16.2bis.

37. The Vendor shall inform IAB Europe immediately of any changes to its processing activities.

    applicable regulations: TCF Policies 10.5.

38. The Vendor shall comply with all other IAB Europe regulations in the Policies and associated documentations.

    applicable regulations: TCF Policies 11.1.