

CamScan

Privacy Policy

Effective Date: May 1, 2020

Last Updated: May 31, 2020

In this Privacy Policy, we inform you about which personal data we collect in the context of your use of TapScan for which purposes your data is used.

1. Contact

The company within the meaning of the data protection laws is:

Artep Media Development SRL
48 Mihai Eminescu, Targu Mures
547329 Mures
Romania

If you have any questions, feel free to contact us at
office@artep.eu

2. Subject matter of data protection

The subject matter of data protection is personal data. Under Article 4(1) GDPR, this means any information relating to an identified or

identifiable natural person; this comprises, for example, names or identification numbers.

3. Collection and use of your data

3.1. Automated data collection

When you access our website, your device will automatically transmit data for technical reasons. These data will be stored separately from other data that you may transmit to us:

- date and time of the access,
- browser type/version,
- operating system used,
- URL of the previously visited website,
- IP address (truncated by one octet)

This data is stored exclusively for technical reasons and will never be assigned to any specific person.

3.2. Support requests

If you contact our support, we will collect and store the personal data transmitted by you for the purpose of processing your request. You are not obligated to provide personal data in your request, and you may contact us with a pseudonym at any time.

We will store your support requests for a period of 120 days from completion of your request, in order to ensure that your request has been successfully processed, and to enable us to understand which

problems may have occurred in the past in the event of subsequent requests that may help with solving your request.

We collect and process your data in order to answer your support request and in order to ensure defect-free operation of our product for you, Article 6(1) point (b) GDPR. If you contact us independently of a specific support request or a technical issue, we will collect and process your personal data based on our legitimate interest in being able to answer email queries and due to the fact that your interests are not overriding, Article 6(1) point (f) GDPR.

5. Cookies

We store so-called "cookies" in order to offer you all features of our website, and to make the use of our websites more convenient. Cookies are small files that are stored on your computer using your internet browser. If you do not want cookies to be used, you can prevent storage of cookies on your device by making the corresponding settings in your internet browser. Please note that the scope of features of our website may be restricted due to this.

We specifically use the following cookies:

- cookies from Firebase;
- a cookie from Google Ads to measure success of Google Ads;
- two cookies from Google Analytics for statistical evaluation of the use of the website and for improvement of our offer;
- a cookie to record whether you have already confirmed the cookie notice with OK;
- a cookie to determine whether the non-standard fonts that are used on the website have been loaded.

These cookies cannot identify you as a person. In any case, use of cookies is justified based on our legitimate interest in demand-oriented design, as well as statistical evaluation of our website, and the fact that your legitimate interests are not overriding, Article 6(1) point (f) GDPR.

6. Transfer of data

In principle, your personal data will only be passed on without your explicit prior consent in the following cases:

6.1. If necessary, to investigate illegal use of our services, or for prosecution, personal data will be passed on to the law-enforcement authorities and potentially to harmed third parties. However, this will only be the case if there are any specific indications of illegal or abusive behavior. Data may also be passed on if this serves to enforce terms and conditions of use or other agreements. We are also legally required to provide information to certain public bodies on request. These are law-enforcement authorities, public authorities that pursue administrative offences subject to fines and the tax authorities.

These data are passed on based on our legitimate interest in fighting abuse, prosecuting criminal offences and the securing, assertion and enforcement of claims and that your rights and interests in protection of your personal data are not overriding, Article 6(1) point (f) GDPR or based on a legal obligation in accordance with Article 6(1) point (c) GDPR.

6.2. We depend on contractually bound third-party companies and external service providers for rendering our services ("Data Processors"). In such cases, personal data will be passed on to such Data Processors in order to permit further processing by them. We select our Data Processors with care and review them at regular intervals to ensure that your rights and freedoms are respected. The Data Processors must only use the data for the purposes specified by us, and are furthermore contractually obligated by us to treat your data only in accordance with this Privacy Policy, and the applicable data protection laws.

In detail, we use the following Data Processors:

- Google LLC (Google Analytics, Google Ads, reCaptcha v3, Firebase)

Data is passed on to Processors based on Article 28(1) GDPR, alternatively based on our legitimate interest in economic and technical advantages connected to the use of specialized processors, and the fact that your rights and interests in protection of your personal data are not overriding, Article 6(1) point (f) GDPR.

6.3. We also process your data in states outside of the European Economic Area ("EEA").

For the USA, the European Commission resolved by its decision dated 12 July 2016 that there is an adequate level of data protection under the provisions of the EU-U.S. Privacy Shield (adequacy decision, Article 45 GDPR). We use the following service providers that are certified under the EU-U.S. Privacy Shield:

- Google LLC

6.4. Within the scope of further development of our business, the structure of doo GmbH may be changed by amending the legal form or by founding, purchasing, or selling subsidiaries, company parts or components. In such transactions, the customer information will be passed on together with the part of the company to be transferred. Every time personal data are transferred to third parties in the scope described above, we will ensure that this is effected in compliance with this Privacy Policy and the relevant data protection laws.

Any passing on of the personal data is justified by our legitimate interest in adjusting our corporate form to the economic and legal conditions if required and by the fact that your rights and interests in protection of your personal data are not overriding, Article 6(1) point (f) GDPR.

7. Change of Purposes

Processing of your personal data for any other purposes than those described shall only take place to the extent that this is permitted by law, or if you have consented to the changed purpose of the processing activities. In case of further processing for other purposes than those for which the data was initially collected, we will inform you about such other purposes before further processing, and provide you with all other information relevant for such.

8. Erasure of your data

We erase or anonymise your personal data as soon as we no longer need them for the purposes for which we have collected or used them according to the above items. As a rule, we store your personal data for the duration of the usage or contractual relationship concerning the website, plus a period of sixty (60) days in which we keep backup copies after erasure. In particular, we will erase your data after the periods described below in the following cases:

- Google Analytics: 14 months.

After the end of these periods, the data will be deleted, except if the data is needed for a longer period due to statutory archiving periods, for criminal prosecution or to secure, assert or enforce legal claims. In such a case, the data will be blocked and is no longer available for further use.

9. COPPA

The Children's Online Privacy Protection Act ("COPPA") is a United States federal law enacted to give parents increased control over what information is collected from their children online and how such information is used. The law applies to websites and services directed to, and which knowingly collect information from, children under the age of 13. Our products and services are not directed to children under the age of 13, nor do we knowingly collect information from children under the age of 13. If you are under the age of 13, please do not provide personal information of any kind whatsoever to TapScan. If a child provides us with personal

information, a parent or legal guardian of that child may contact us to obtain that information and/or delete it from our records by sending an email to tapscanapp@gmail.com

10. Changes to this privacy policy

We may make changes to this Privacy Policy (and/or other applicable policies and Addenda) as the applicable laws, relevant technologies, and our data processing practices change. We will notify you of changes to this Privacy Policy (and/or other applicable policies and Addenda) by posting the updated policy on our website and in our applications and other products and services. The changes to this Privacy Policy (and/or other applicable policies and Addenda) shall become effective upon such posting (as indicated by the date following "Last Updated:" at the top of this Privacy Policy and/or other applicable policies and Addenda), or as otherwise required by applicable law. We encourage you to review this Privacy Policy (and other applicable policies and Addenda) on a periodic basis.