stashcat®

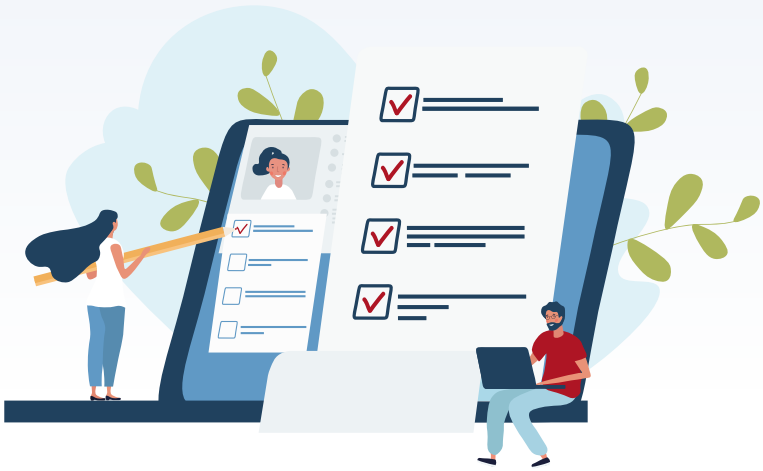
GDPR

GENERAL DATA PROTECTION REGULATION

WHITEPAPER

How to check your software for GDPR compliance

Table of contents



Use our quick check list to review the most important criteria to assess whether a software or service can be GDPR compliant.

quick check list

Is personal data processed?

The term „personal data" is defined in Art. 4 No. 1 of the General Data Protection Regulation. According to this, personal data is any information that relates to an identified or identifiable person. If the data allows a link to be established between the information and a person, the information falls under this term. [1] [2]

Recommended action

Take a look at the terms of use, the privacy policy and, if available, also the record of processing activities and the data processing agreement (DPA).If personal data is collected, it is essential to check the following questions to minimize risks.

On Page 5

Do third parties have access to the personal data?

If a provider passes on personal data to a „third party", it is obliged to make this apparent in writing. In the data processing agreement (DPA), the contractor has to commit to only process the data in accordance with the order and as instructed.

If, for example, usage data is collected via an online tracking tool without first obtaining consent, this data is considered to be incorrectly collected under data protection law. In this case, the data may not be used and must be deleted. [3] [4] [5]

Recommended action

If third parties are allowed access to personal data, the provider is obliged to inform about this. Take a look at the privacy policy and, if available, at the record of processing activities and the DPA for a list of data that is passed on to third parties.

If the provider manages data in insecure third countries or shares it with additional partners in insecure third countries (see „Is data transferred to third countries?"), we recommend against using the service.

On Page 5

Is data transferred to third countries?

Third countries are defined as countries outside the EU and the European Economic Area (or the United Kingdom) where the software is offered or operated. According to the GDPR, the processing of personal data outside the EU is prohibited unless there is an appropriate level of data protection in the third countries (Art. 44 to 49 GDPR).

The following countries have an appropriate level of data protection outside the EU: Andorra, Argentina, Canada (commercial organizations only), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and Japan.

The following countries **do not** have an appropriate level of data protection: Australia, Brazil, China, India, Mexico, Russia, Singapore, South Korea, Ukraine, and the United States.

In July 2020, the European Court of Justice declared the "EU-US Privacy Shield Agreement" invalid, which stipulated that US companies could undertake to comply with EU law. Whether data can be transferred to the United States is therefore currently disputed, as possible access to personal data by US authorities cannot be ruled out. According to the European Court of Justice, there is therefore no sufficient level of protection.

It is recommended to refrain from using U.S. services until the legal situation is clarified. [5] [6] [7]

Recommended action

Check the privacy policy and, if available, the record of processing activities and the DPA to see whether data is processed in third countries. Data is not allowed to be processed outside the EU and the European Economic Area, nor outside countries with an adequate level of data protection. If this is nevertheless the case, refrain from using the software or service in order to reduce risks.

On Page 5

Does the product collect and process only necessary data?

Basically, the software should ensure data protection through technical design and data protection-friendly default settings and thus only process the data that is actually required (Art. 25 GDPR). The responsible software operator is thus required to implement appropriate technical and organizational measures (abbreviation TOM) in a timely manner so that data protection is implemented in accordance with the GDPR.

In the case of data protection-friendly default settings, the collection of personal data should be minimized and only data that is actually required should be collected. In addition, the software manufacturer should be transparent about the function and processing of personal data. [3] [8]

Recommended action

Check the privacy policy and, if available, also the record of processing activities and the DPA to see which data are actually processed. In these documents, ensure that by default only personal data whose processing is necessary for the respective specific processing purpose is being processed.

On Page 5

Are technical security measures in place to ensure secure processing of personal data?

With regard to security, check whether the software has sufficiently high technical and organizational measures in place to ensure the secure processing of personal data (Art. 32 GDPR). The software has to ensure data protection through technical design and data protection-friendly default settings. Technical default settings should therefore have been made in such a way that they comply with data protection from the outset. Has the state of the art been taken into account? [3] [9]

Recommended action

All information on the measures that the provider maintains at the technical and organizational level can be found in the "technical and organizational measures" (TOM). These are part of and/or annexed to the DPA.

With the measures described there, the provider must ensure an appropriate level of protection. The level of protection must prevent risks that may occur during processing (e.g. destruction, loss or modification of data).The provider also has to ensure that persons with access to your data (e.g. employees of the provider) only process it on instruction.

As a clue, you can search these texts for terms such as "pseudonymization" or "encryption". Read to see if measures related to the availability and resilience of the systems are recorded. Does the provider describe how the system will be restored after an incident? If you cannot find a TOM at all or if it does not describe measures for any of the points mentioned, you should, if necessary, refrain from using the service or commission a specialist to check it. [13]

On Page 5

Does the operator fulfill his duty to provide information?

The software operator has to make it possible to provide information about stored data and thus fulfill his duty to inform. The customers have a right to be informed about personal data (Art. 15 GDPR). This includes processing purposes, planned duration for storage or which recipients have access to the data. [3] [10]

Recommended action

Check the privacy policy and, if available, the DPA to see how the software operator fulfills its duty to inform.

Is the right to delete personal data respected?

The right to delete personal data is based on the principle of storage limitation (Art. 5 GDPR) and the right to be forgotten (Art. 17 GDPR). The principle states that personal data collected for a specific purpose are no longer necessary after this purpose has been fulfilled and must therefore be deleted (unless otherwise required by law). Regarding the purpose for which the data is used, this is important because data controllers are only allowed to store personal data for as long as it is necessary for the processing purpose to identify you. If the purpose is inadmissible, time-barred or the contractual relationship has ended, the data must be deleted by the responsible party. [11] [12]

Recommended action

If you would like to request deletion of your data, the best way to do so is to contact the responsible parties by e-mail or mail. Refer to your right of deletion. You can also find sample letters for requesting this online, for example on the website of the consumer advice center.

Not all providers give out all the necessary information where you would expect it. In the recommended action, you will find tips on where you should find the relevant information. If you cannot find the information or documents on the relevant pages of the providers, have a look at the legal notice of the operator for contact details and obtain the desired information.

List of sources

1. https://dsgvo-gesetz.de/themen/personenbezogene-daten
2. https://www.datenschutz.org/personenbezogene-daten
3. https://www.datenschutz-praxis.de/datenschutzbeauftragte/so-pruefen-sie-software-auf-dsgvo-konformitaet
4. https://eu-datenschutz-grundverordnung.net/dritter
5. https://t3n.de/news/dsgvo-daten-rechtssicher-weitergeben-853271
6. https://dsgvo-gesetz.de/themen/drittland
7. https://legal.trustedshops.com/login
8. https://eu-datenschutz-grundverordnung.net/datenschutz-durch-technikgestaltung-und-voreinstellungen
9. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/technische-richtlinien_node.html
10. https://dsgvo-gesetz.de/art-15-dsgvo
11. https://www.verbraucherzentrale.de
12. https://www.datenschutz-praxis.de/tom/empfehlungen-tuev-daten-sicher-loeschen
13. https://dsgvo-gesetz.de/art-32-dsgvo

stashcat GmbH
Hamburger Allee 2-4 | 30161 Hannover | +49 (0) 511 - 67 51 90
hello@stashcat.com | www.stashcat.com