stashcat®

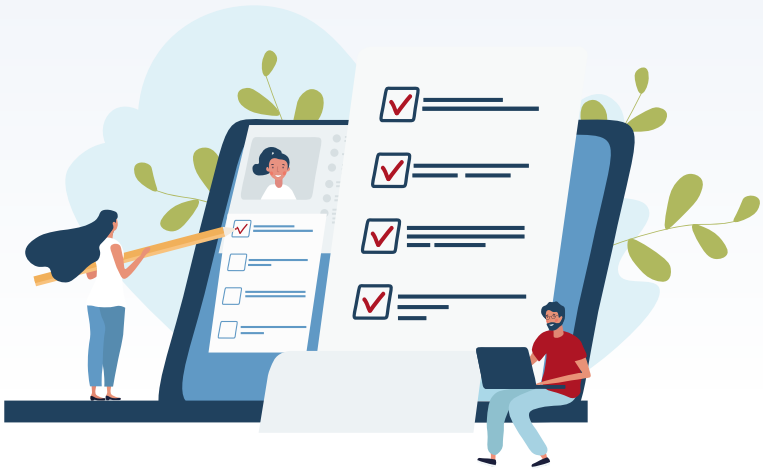
DSGVO

DATENSCHUTZ GRUNDVERORDNUNG

WHITEPAPER

So können Sie Ihre Software auf DSGVO-Konformität prüfen

Inhaltsverzeichnis



Nutzen Sie unsere Quickcheck-Liste zur Prüfung der wichtigsten Kriterien, um einzuschätzen, ob eine Software oder ein Dienst DSGVO-konform sein kann.

Checkliste

Werden personenbezogene Daten verarbeitet?

Der Begriff „personenbezogene Daten" wird in Art. 4 Nr. 1 der Datenschutz-Grundverordnung definiert. Danach sind personenbezogene Daten alle Informationen, welche sich auf eine identifizierte oder identifizierbare Person beziehen. Lässt sich durch die Daten eine Verbindung zwischen der Information und einer Person herstellen, fallen die Informationen unter diesen Begriff. [1] [2]

Handlungsempfehlung

Schauen Sie in die Nutzungsbedingungen, die Datenschutzerklärung und falls diese vorliegen auch in das Verarbeitungsverzeichnis und den Vertrag zur Auftragsverarbeitung (AV-Vertrag). Werden personenbezogene Daten erfasst, ist die Prüfung der folgenden Fragen unbedingt notwendig, um Risiken zu vermindern.

ⓘ Auf Seite 5

Haben Dritte Zugriff auf die personenbezogenen Daten?

Wenn ein Anbieter personenbezogene Daten an einen „Dritten“ weitergibt, ist er verpflichtet, dies schriftlich erkennbar zu machen. In einem Vertrag zur Auftragsverarbeitung (AV-Vertrag) muss sich der Auftragnehmer dazu verpflichten, die Daten nur entsprechend dem Auftrag und nach Weisung zu verarbeiten.

Wenn zum Beispiel über ein Online-Trackingtool Nutzungsdaten erfasst werden, ohne vorher eine Einwilligung einzuholen, gelten diese Daten als datenschutzrechtlich nicht korrekt erhoben. Die Daten dürfen in diesem Fall nicht genutzt und müssen gelöscht werden. [3] [4] [5]

Handlungsempfehlung

Wird Dritten der Zugriff auf personenbezogene Daten gestattet, ist der Anbieter verpflichtet, darüber zu informieren. Schauen Sie hierzu in der Datenschutzerklärung und falls diese vorliegen auch in dem Verarbeitungsverzeichnis und dem Vertrag zur Auftragsverarbeitung (AV-Vertrag) nach einer Auflistung von Daten, die an Dritte weitergegeben werden.

Werden durch den Anbieter Daten in unsicheren Drittländern verwaltet oder mit weiteren Partnern in unsicheren Drittländern geteilt (siehe „Werden Daten in Drittländer übermittelt?“), empfehlen wir von der Nutzung des Dienstes abzusehen.

ⓘ Auf Seite 5

Werden Daten in Drittländer übermittelt?

Man spricht von sogenannten Drittländern, wenn die Software außerhalb der EU und des europäischen Wirtschaftsraums (oder des Vereinigten Königreichs) angeboten bzw. betrieben wird. Die Verarbeitung personenbezogener Daten ist laut der DSGVO außerhalb der EU verboten, sofern in den Drittländern kein angemessenes Datenschutzniveau herrscht (Art. 44 bis 49 DSGVO).

In folgenden Ländern herrscht ein angemessenes Datenschutzniveau außerhalb der EU: Andorra, Argentinien, Kanada (nur kommerzielle Organisationen), Färöer-Inseln, Guernsey, Israel, Isle of Man, Jersey, Neuseeland, Schweiz, Uruguay und Japan.

In folgenden Ländern herrscht **kein** angemessenes Datenschutzniveau: Australien, Brasilien, China, Indien, Mexiko, Russland, Singapur, Südkorea, Ukraine und USA.

Der Europäische Gerichtshof erklärte im Juli 2020 das „EU-USA-Privacy-Shield-Abkommen“ für unwirksam, in dem geregelt war, dass US-Unternehmen sich verpflichteten konnten das EU-Recht zu beachten. Ob eine Datenweitergabe in die USA erfolgen kann ist somit aktuell strittig, da mögliche Zugriffe auf personenbezogene Daten durch US-Behörden nicht ausgeschlossen werden können. Laut Europäischem Gerichtshof liegt deshalb gerade kein ausreichendes Schutzniveau vor.

Um jegliches rechtliches Risiko zu vermeiden, empfehlen wir, bis zur Klärung der Rechtslage auf die Nutzung von US-Diensten zu verzichten. [5] [6] [7]

Handlungsempfehlung

Schauen Sie in der Datenschutzerklärung und falls diese vorliegen auch in dem Verarbeitungsverzeichnis und dem Vertrag zur Auftragsverarbeitung (AV-Vertrag) nach, ob Daten in Drittländern verarbeitet werden. Daten dürfen weder außerhalb der EU und des europäischen Wirtschaftsraums noch außerhalb von Ländern mit angemessenem Datenschutzniveau verarbeitet werden. Sollte dies dennoch der Fall sein, verzichten Sie auf die Nutzung der Software oder des Dienstes.

ⓘ Auf Seite 5

Erhebt und verarbeitet das Produkt nur erforderliche Daten?

Grundsätzlich sollte die Software Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellung gewährleisten und somit nur die tatsächlich erforderlichen Daten verarbeiten (Art. 25 DSGVO). Der verantwortliche Softwarebetreiber wird also aufgefordert, rechtzeitig geeignete technische und organisatorische Maßnahmen (Abkürzung TOM) umzusetzen, sodass der Datenschutz im Sinne der DSGVO umgesetzt wird.

Bei den datenschutzfreundlichen Voreinstellungen sollte die Erfassung personenbezogener Daten minimiert sein und nur tatsächlich erforderliche Daten erfasst werden. Zudem sollte der Softwarehersteller transparent mit der Funktion und Verarbeitung personenbezogener Daten umgehen. [3] [8]

Handlungsempfehlung

Schauen Sie in der Datenschutzerklärung und falls diese vorliegen auch in dem Verarbeitungsverzeichnis und dem Vertrag zur Auftragsverarbeitung (AV-Vertrag) nach, welche Daten tatsächlich verarbeitet werden. Stellen Sie in diesen Dokumenten sicher, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich sind, verarbeitet werden.

Auf Seite 5

Sind technische Sicherheitsmaßnahmen vorhanden, um eine sichere Verarbeitung der personenbezogenen Daten zu gewährleisten?

Prüfen Sie im Bezug auf die Sicherheit, ob bei der Software ausreichend hohe technisch-organisatorische Maßnahmen vorhanden sind, um die sichere Verarbeitung der personenbezogenen Daten zu gewährleisten (Art. 32 DSGVO). Die Software sollte Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellung sicherstellen. Technische Voreinstellungen sollten also so vorgenommen worden sein, dass sie von Anfang an der Datenschutz-Verordnung entsprechen.

Ist der Stand der Technik berücksichtigt (z. B. die Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik – kurz BSI)? Das Ziel der technischen Richtlinien des BSI ist die Verbreitung von angemessenen IT-Sicherheitsstandards. [3] [9]

Handlungsempfehlung

Alle Angaben zu den Maßnahmen, welche der Anbieter auf technischer und auf organisatorischer Ebene vorhält, finden Sie in den „technischen und organisatorischen Maßnahmen“ (TOM). Diese sind Bestandteil und/oder Anlage des Vertrags zur Auftragsverarbeitung (AV-Vertrag).

Mit den dort beschriebenen Maßnahmen muss der Anbieter ein angemessenes Schutzniveau sicherstellen. Das Schutzniveau muss Risiken vorbeugen, welche bei der Verarbeitung auftreten können, wie zum Beispiel Vernichtung, Verlust oder Veränderung der Daten. Der Anbieter muss mit diesen Festlegungen zudem sicherstellen, dass Personen mit Zugang zu Ihren Daten (zum Beispiel Mitarbeiter des Anbieters) diese nur auf Anweisung verarbeiten.

Als Anhaltspunkt können Sie in diesen Texten unter anderem nach Begriffen wie „Pseudonymisierung“ oder „Verschlüsselung“ suchen. Lesen Sie nach, ob Maßnahmen im Zusammenhang mit der Verfügbarkeit und Belastbarkeit der Systeme festgehalten sind. Schildert der Anbieter, wie das System nach einem Zwischenfall wiederhergestellt wird? Sollten Sie gar keine TOM finden oder sollten diese zu keinem der genannten Punkte Maßnahmen beschreiben, sollten Sie von der Nutzung des Dienstes absehen oder einen Fachmann zurate ziehen. [13]

Auf Seite 5

Kommt der Betreiber seiner Informationspflicht nach?

Der Softwarebetreiber hat dafür Sorge zu tragen, Auskunft über gespeicherte Daten zu geben und somit seiner Informationspflicht nachzukommen. Kunden haben nämlich ein Auskunftsrecht über personenbezogene Daten (Art. 15 DSGVO). Darunter fallen unter anderem Verarbeitungszwecke, geplante Dauer für die Speicherung oder welche Empfänger Zugriff auf die Daten haben. [3] [10]

Handlungsempfehlung

Schauen Sie in der Datenschutzerklärung und falls dieser vorliegt auch in dem Vertrag zur Auftragsverarbeitung (AV-Vertrag) nach, wie der Softwarebetreiber seiner Informationspflicht nachgeht.

Wird das Recht personenbezogene Daten zu löschen beachtet?

Das Recht personenbezogene Daten zu löschen basiert auf dem Grundsatz der Speicherbegrenzung (Art. 5 DSGVO) und dem Recht auf Vergessenwerden (Art. 17 DSGVO). Der Grundsatz besagt, dass personenbezogene Daten, die für einen bestimmten Zweck erhoben wurden nach Erfüllung dieses Zweckes nicht mehr erforderlich sind und damit zu löschen sind (sofern kein weiteres rechtliches Vorgeben dem entgegensteht). Der Verwendungszweck der Daten spielt eine wichtige Rolle, denn die Verantwortlichen dürfen personenbezogene Daten nur so lange speichern, wie es für den Verarbeitungszweck zur Identifikation Ihrer Person notwendig ist. Ist der Zweck unzulässig, verjährt oder das Vertragsverhältnis beendet, so sind die Daten vom Verantwortlichen zu löschen. [11] [12]

Handlungsempfehlung

Möchten Sie beantragen, dass Ihre Daten gelöscht werden, wenden Sie sich per E-Mail oder Brief an die Verantwortlichen. Beziehen Sie sich auf Ihr Recht der Löschung. Sie finden online auch Musterbriefe zur Beantragung, beispielsweise auf der Website der Verbraucherzentrale.

Nicht alle Anbieter geben alle notwendigen Informationen dort aus, wo sie zu erwarten wären. In der Handlungsempfehlung finden Sie Tipps dazu, wo Sie die entsprechenden Informationen finden sollten. Können Sie die Informationen oder Dokumente nicht auf den entsprechenden Seiten der Anbieter finden, schauen Sie im Impressum des Betreibers nach Kontaktdaten und holen Sie sich die gewünschten Informationen ein.

Quellenverzeichnis

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