www.jusletter-it.eu

Simon Schlauri

Auftragsdatenverarbeitung nach DSGVO

Category: News
Region: Switzerland
Field of law: Data Protection

Citation: Simon Schlauri, Auftragsdatenverarbeitung nach DSGVO, in: Jusletter IT 24-Mai-2018

[Rz 1] Am 25. Mai 2018 wird die europäische Datenschutz-Grundverordnung (DSGVO) wirksam. Schweizer Unternehmen, die Daten von Personen mit Aufenthalt in der EU verarbeiten, fallen unter deren neue Regelungen, sofern sie diesen Personen Waren oder Dienstleistungen anbieten oder deren Verhalten in der EU beobachten (Art. 3 Abs. 2 DSGVO). Betroffen sind damit insbesondere auch Schweizer Unternehmen, die als Subunternehmen Daten im Auftrag von Anbietern in der EU verarbeiten. Was gilt es dabei zu beachten?

[Rz 2] Nach Art. 4 Nr. 8 DSGVO ist ein Auftragsverarbeiter eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des verantwortlichen Unternehmens verarbeitet.

[Rz 3] Zentral ist dabei, dass der Auftragsverarbeiter die Daten nur auf Weisung des Verantwortlichen verarbeiten darf (Art. 29 DSGVO). Er darf bei der Verarbeitung also keine eigenen Interessen oder gar Interessen Dritter verfolgen. Die Tätigkeit einer Kreditauskunftei, die Daten von ihren Auftraggebern zentral sammelt und in der Folge auch weiteren angeschlossenen Unternehmen zur Verfügung stellt, wäre damit keine Auftragsverarbeitung im Sinne des Gesetzes. Eine Weitergabe an sie bedürfte denn auch eines gesonderten Rechtfertigungsgrundes, wie beispielsweise einer Einwilligung der betroffenen Person.

[Rz 4] Die eigentliche Auftragsverarbeitung im einzigen Interesse des Verantwortlichen ist demgegenüber ohne Einwilligung der betroffenen Person zulässig. Vorausgesetzt ist einzig, dass die betroffene Person über die Weitergabe an Auftragsverarbeiter informiert wird, beispielsweise im Rahmen einer Datenschutzerklärung.[1]

[Rz 5] Aus Perspektive des verantwortlichen europäischen Auftraggebers ist insbesondere Art. 28 DSGVO von Bedeutung. Der Auftragsverarbeiter muss dem verantwortlichen Auftraggeber gegenüber nämlich vertraglich garantieren, die Vorgaben der DSGVO einzuhalten.

[Rz 6] Art. 28 DSGVO zählt Inhalte auf, die der Vertrag zwischen verantwortlichem Unternehmen und Auftragsverarbeiter zwingend aufweisen muss. Dazu gehört insbesondere Folgendes:

- Gegenstand, Dauer, Art und Zweck der Verarbeitung.
- Art der personenbezogenen Daten (Beispiel: Gesundheitsdaten).
- Kategorien betroffener Personen (Beispiel: private Kunden, Ärzte).
- Der Auftragsverarbeiter darf nur auf dokumentierte Weisung des Verantwortlichen hin tätig werden. (Die Inhalte solcher Weisungen sind dabei selbstverständlich durch den vertraglichen Rahmen begrenzt.) Geht der Auftragsverarbeiter davon aus, dass eine Weisung die DSGVO verletzt, so informiert er zudem den Verantwortlichen darüber.
- Der Auftragsverarbeiter darf ohne schriftliche Genehmigung keine Unterauftragsverarbeiter zuziehen. Zulässig ist jedoch eine allgemeine Genehmigung, sofern der Auftragsverarbeiter verpflichtet bleibt, den Verantwortlichen über neue Unterverarbeiter zu informieren.
- Beigezogene Personen (insb. Mitarbeiter) müssen sich zur Vertraulichkeit verpflichten oder einer gesetzlichen Verschwiegenheitspflicht unterstehen.
- Die Datensicherheitsvorschriften von Art. 32 DSGVO sind einzuhalten (Beispiele: Verschlüsselung, Zugangsschutz, Datenwiederherstellung).
- Der Auftragsverarbeiter muss das verantwortliche Unternehmen nach Möglichkeit dabei unterstützen, die Rechte der betroffenen Personen zu erfüllen (Beispiele: Recht auf Aus-

[1] Gernot Sydow (Hrsg.), Handkommentar Europäische Datenschutzgrundverordnung, Dike Verlag, Zürich 2017, N 19 zu Art. 13.

kunft, Recht auf Löschung) und die weiteren Pflichten des verantwortlichen Unternehmens nach DSGVO zu verfolgen (Beispiel: Pflicht zur Meldung von Daten-Leaks an Behörden binnen 72 Stunden).
- Der Auftragsverarbeiter muss die Daten nach dem Ende der Verarbeitung löschen oder zurückgeben.
- Der Auftragsverarbeiter muss dem Verantwortlichen gegenüber die Erfüllung seiner Pflichten schriftlich nachweisen können und Inspektionen zulassen.

[Rz 7] Der Vertrag über die Auftragsverarbeitung ist schriftlich abzuschliessen, was sich explizit aus der DSGVO, aber auch schon aus der allgemeinen Dokumentationspflicht der DSGVO ergibt.

[Rz 8] Der Auftragsverarbeiter muss auch die gemäss DSGVO zwingend vorgegebenen vertraglichen Aufgaben selbstverständlich nicht kostenlos erbringen; denkbar ist etwa eine Verrechnung im Stundensatz.

[Rz 9] Die Verarbeitung durch Auftragsverarbeiter ausserhalb der EU untersteht weiteren Vorgaben von Art. 44 ff. DSGVO, so ist beispielsweise die Verwendung der Standardklauseln der EU-Kommission für grenzüberschreitenden Datenverkehr zu empfehlen.

[Rz 10] Nachdem die Inhalte des Auftragsverarbeitungsvertrags ohnehin gesetzlich vorgegeben sind, kann es sich für Auftragsverarbeiter in der Schweiz lohnen, bereits im Lauf von Vertragsverhandlungen darauf hinzuweisen, dass man bereit ist, einen DSGVO-konformen Auftragsverarbeitungsvertrag abzuschliessen bzw. einen entsprechenden Anhang in den Vertrag einzubinden. Umgekehrt sehe ich es jeweils als schlechtes Omen, wenn eine von einem Auftragsverarbeiter vorgelegte Vertragsversion mit keinem Wort auf deren neue Pflichten nach DSGVO eingeht; der Schluss liegt in einem solchen Fall nahe, dass das Unternehmen sich noch nicht hinreichend mit diesen Pflichten auseinandergesetzt hat, und dass seine Datenverarbeitung damit auch sonst nicht gesetzeskonform sein könnte.

Simon Schlauri