Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Grundsätze zum Datenschutz

1. Sorgfalt

Art. 5 der Datenschutz-Grundverordnung (DSGVO) enthält eine Reihe von Grundsätzen, die Sie einhalten müssen, wenn Sie personenbezogene Daten verarbeiten. Sowohl der Begriff der personenbezogenen Daten als auch der Begriff der Verarbeitung sind sehr weit gefasst: Für einen **Personenbezug** genügt es, dass Dritte über Mittel verfügen, die Daten einem Menschen (der „betroffenen Person") zuzuordnen. So sind beispielsweise IP-Adressen oft personenbezogene Daten, weil etwa über den Internetanbieter herausgefunden werden kann, wem der Anschluss gehört. **Verarbeitung** meint alle Vorgänge im Zusammenhang mit personenbezogenen Daten – dies sogar, wenn sie ohne automatisierte Verfahren erfolgen.

➔ Voraussetzung, um diese Grundsätze einhalten zu können, ist, dass Sie im Detail wissen, in welchen Situationen Sie welche personenbezogenen Daten wie verarbeiten. Hier sollten Sie von Anfang an sorgfältig arbeiten.

2. Rechtmäßigkeit

Wenn Sie personenbezogene Daten verarbeiten, benötigen Sie dafür eine **Rechtsgrundlage** (Art. 6 DSGVO). Beispielsweise sind alle Datenverarbeitungen erlaubt, die für die Erfüllung eines Vertrags zwischen Ihnen und der betroffenen Person – also der Person, auf die die Daten sich beziehen – **zwingend notwendig** sind. Gleiches gilt für alle Datenverarbeitungen, zu denen Sie etwa aus steuerrechtlichen Gründen verpflichtet sind. In vielen Fällen gibt Ihnen auch eine **Interessenabwägung** eine Rechtsgrundlage – etwa wenn eine Datenverarbeitung nicht für die Vertragserfüllung nötig, aber doch sinnvoll und kaum belastend ist. Und natürlich können Sie sich eine **Einwilligung** in die Datenverarbeitung geben lassen. Beachten Sie aber bitte die **gesetzlichen Voraussetzungen**, damit die Einwilligung auch wirksam ist (Art. 4 Nr. 11, Art. 6 Abs. 1 Uabs. 1 lit. a, Art. 7, ggf. Art. 8, ggf. Art. 9 Abs. 2 lit. a, ggf. Art. 22 Abs. 2 lit. c, Abs. 3, Abs. 4, ggf. Art. 49 Abs. 1 lit. a DSGVO).

➔ Eine Einwilligung ist allerdings nicht die richtige Rechtsgrundlage, wenn Ihr Unternehmen auf eine bestimmte Datenverarbeitung angewiesen ist, alleine schon deshalb, weil die betroffene Person ihre Einwilligung jederzeit widerrufen kann.

Für besonders geschützte Daten (wie beispielweise Gesundheitsdaten) gelten Einschränkungen (Art. 9 DSGVO). Wenn Sie **externe Dienstleister** einschalten, brauchen Sie für die Weitergabe an den Dienstleister keine gesonderte Rechtsgrundlage, wenn Sie mit dem Dienstleister einen den gesetzlichen Mindestanforderungen entsprechenden **Auftragsverarbeitungsvertrag** abschließen (Art. 28 DSGVO). Der Dienstleister wird dann so behandelt, als wäre er ein Teil Ihres Unternehmens.

3. Treu und Glauben

Personenbezogene Daten dürfen Sie nur nach Treu und Glauben verarbeiten. Das bedeutet einerseits, dass Sie Ihre Datenverarbeitung **transparent** machen müssen (siehe 4. Transparenz). Andererseits dürfen Sie die betroffenen Personen auch **nicht überraschen**. Beispiel: Sie dürfen grundsätzlich nicht eine Einwilligung einholen und nach einem Widerruf der Einwilligung auf eine andere Rechtsgrundlage umschwenken, um die Daten weiterhin zu verarbeiten. Denn bei der Erhebung der Daten haben Sie den Eindruck erweckt, die betroffene Person habe es in der Hand, die Datenverarbeitung durch Widerruf ihrer Einwilligung zu beenden.

➔ Wenn Sie zwei Rechtsgrundlagen nutzen wollen, müssen Sie dies von Anfang an transparent machen. Ein späterer Wechsel verstößt regelmäßig gegen Treu und Glauben.

4. Transparenz

Betroffene Personen sollen nach der DSGVO grundsätzlich immer wissen, wer welche Daten über sie zu welchem Zweck und wie lange verarbeitet. Deshalb haben Sie verschiedene **Informationspflichten** (insbesondere Art. 13 und 14 DSGVO). Diese Informationspflichten müssen Sie von sich aus erfüllen. Besonders wichtig ist Transparenz, wenn Sie eine **Einwilligung** einholen wollen. Denn Einwilligungen sind nur wirksam, wenn sie (neben weiteren Anforderungen) in **Kenntnis der Sachlage, spezifisch und unmissverständlich** erteilt werden. Auf Anfrage müssen Sie betroffenen Personen zudem **Auskunft** über sämtliche zu ihnen verarbeiteten Daten und diverse weitere Informationen erteilen (Art. 15 DSGVO).

➔ All diese Pflichten können Sie nur erfüllen, wenn Sie genau wissen, welche Daten Sie zu welchem Zweck, wie, wo und wie lange verarbeiten – wenn Ihre Datenverarbeitungen also auch für Sie transparent sind.

Diese Transparenz hinsichtlich Ihrer Datenverarbeitungen ist zudem Voraussetzung, um Ihre weiteren gesetzlichen Pflichten einzuhalten. Entsprechend schreibt Art. 30 DSGVO vor, dass Sie ein sogenanntes **Verzeichnis von Verarbeitungstätigkeiten** anlegen.

5. Zweckbindung

Bevor Sie mit der Verarbeitung personenbezogener Daten beginnen, müssen Sie die **Zwecke** der Verarbeitung **eindeutig und präzise festlegen** und dokumentieren. Diese Zwecke müssen legitim sein, insbesondere rechtmäßig. Die Daten dürfen nur zu den konkret festgelegten Zwecken verarbeitet werden. Spätere Zweckänderungen sind nur sehr begrenzt zulässig.

➔ Im Rahmen Ihrer Transparenzpflichten müssen Sie die betroffenen Personen über die Zwecke der Datenverarbeitung informieren.

6. Datenminimierung

Sie dürfen nur so viele personenbezogene Daten verarbeiten, wie dies für die festgelegten Zwecke **notwendig** ist – es darf also ohne diese Daten „nicht gehen". Außerdem dürfen Sie nur Daten verarbeiten, die für den Zweck **erheblich** sind.

➔ Zusätzlich müssen Sie die Verhältnismäßigkeit wahren: Selbst wenn ein bestimmter Zweck wirklich nur mit einer umfangreichen Datenverarbeitung erreichbar ist, kann diese Datenverarbeitung außer Verhältnis zum weniger relevanten Zweck stehen und daher unzulässig sein.

7. Richtigkeit

Personenbezogene Daten müssen richtig und, soweit dies für den jeweiligen Zweck erforderlich ist, **auf dem neuesten Stand** sein.

➔ Soweit Ihr Zweck dies erfordert, müssen Sie Maßnahmen treffen, um unrichtige Daten zu berichtigen oder zu löschen.

8. Speicherbegrenzung

Sie dürfen personenbezogene Daten nur so lange verarbeiten, wie dies für den jeweiligen **Zweck erforderlich** ist. Sobald dieser Zweck erfüllt ist, müssen Sie die Daten löschen.

➔ Hierfür müssen Sie vorab Fristen festlegen, nach denen die Daten gelöscht werden, und Ereignisse, mit denen diese Löschfristen beginnen.

Können Sie ausnahmsweise noch keine festen Löschfristen festlegen, etwa weil sich noch nicht absehen lässt, wie lange bestimmte Daten benötigt werden, müssen Sie festlegen, **wann Sie überprüfen**, ob die Daten immer noch benötigt werden.

9. Integrität und Vertraulichkeit

Werden personenbezogene Daten Unbefugten bekannt, werden sie unzulässig verändert oder gehen sie verloren, kann dies zu schweren **Schäden** für die betroffenen Personen führen (und bei einem Bekanntwerden auch für das verantwortliche Unternehmen).

➔ Sie müssen daher technische und organisatorische Schutzmaßnahmen treffen, um für eine angemessene Sicherheit der Daten zu sorgen.

Die **Schutzmaßnahmen** müssen insbesondere die unbefugte oder unrechtmäßige Verarbeitung, den unbeabsichtigten Verlust, die unbeabsichtigte Zerstörung oder die unbeabsichtigte Schädigung verhindern.

10. Rechenschaftspflicht

Art. 5 Abs. 2 DSGVO erlegt Ihnen die Rechenschaftspflicht für diese Grundsätze auf.

➔ Dies bedeutet, dass Sie jederzeit in der Lage sein müssen, nachzuweisen, dass Sie diese Grundsätze einhalten.

Dabei handelt es sich auch um eine **Beweislastregelung** – und zwar sowohl gegenüber der Aufsichtsbehörde als auch gegenüber den betroffenen Personen. Beispielsweise müssen Sie – wenn die Rechtsgrundlage Ihrer Verarbeitung eine Einwilligung sein soll – nicht nur eine (wirksame) **Einwilligung** einholen, sondern Sie müssen auch **beweisen** können,

(1) dass Sie die Einwilligung überhaupt eingeholt haben,

(2) dass gerade die betroffene Person die Einwilligung abgegeben hat,
(3) dass alle Tatbestandvoraussetzungen der Einwilligung erfüllt sind.

So verstoßen Sie etwa gegen Ihre Rechenschaftspflicht, wenn Sie nicht die Umstände der Einwilligung nachweisen können, etwa dass die betroffene Person frei entscheiden konnte, ob sie zustimmt, dass sie genau wusste, in welche Datenverarbeitung sie einwilligt und dass das, was Sie als Einwilligung behandeln, tatsächlich und unmissverständlich eine eindeutig zustimmende Handlung der betroffenen Person war. Darüber hinaus gibt es in der DSGVO noch viele implizite Beweislastregelungen, etwa durch Formulierungen wie „nur rechtmäßig wenn".

Sie brauchen Unterstützung?

Kostenlose Online-Schulungen der Berliner Beauftragten für Datenschutz und Informationsfreiheit: https://www.datenschutz-berlin.de/themen/unternehmen/start-up-schule/

Weiterführende Links

Datenschutzleitfaden des Europäischen Datenschutzausschuss (EDSA) für Kleinunternehmen: https://edpb.europa.eu/sme-data-protection-guide/home_en

Website der Stiftung Datenschutz zum Datenschutz für Kleinunternehmen: https://ds-kleinunternehmen.de/startseite