Musterverzeichnis

1. Auf einen Blick

In diesem Kapitel wollen wir in Kürze die wichtigsten Konzepte und Schritte auf dem Weg zu einem erfolgreichen Datenschutzkonzept vorstellen. Da die DSGVO für Verstöße einen sehr hohen Strafrahmen vorsieht (bis zu 20 Mio € bzw 4 % des weltweiten Jahresumsatzes), potenzielle Verstöße also existenzbedrohende Geldbußen bedeuten können, ist die Erfüllung der essenziellen Punkte wesentlich. Weiterführende Informationen zu den einzelnen Themen können dem jeweiligen Kapitel in diesem Buch entnommen werden.

Die chronologische Checkliste am Anfang soll helfen, sich einen Step-by-Step-Plan zurechtzulegen und auf einen Blick den Umfang der „Aufgabe Datenschutz" in der ersten Phase eines Unternehmens abschätzen zu können. Darauf folgt ein Überblick über die allernotwendigsten und wichtigsten Pflichten, nennen wir sie Musthaves. Konträr dazu eine kurze Darstellung von vermeidbaren Fehlern, No-Gos, die allesamt in der Unternehmenspraxis vorkommen und das Risiko einer Strafe erhöhen.

1.1. Step-by-Step

Step 1 – Dateninventur

Eine Übersicht darüber erstellen, zu welchen Zwecken das Unternehmen Daten zu verarbeiten plant und welche Daten dafür verarbeitet werden sollen.

Step 2 – Rollenverteilung

Ermitteln, welche Rolle das Unternehmen bei der Datenverarbeitung einnimmt (Verantwortliche, Auftragsverarbeiter, Joint Controller) (Kapitel 2.6.).

Step 3 – Prinzipientreue

Prüfen, ob die geplante Verarbeitung allen Prinzipien (zB Datenminimierung, Rechtmäßigkeit, Transparenz) entspricht (Kapitel 3.1.).

Step 4 – Risikoabschätzung

Einerseits ermitteln, wie risikoreich die Verarbeitung ist, um abschätzen zu können, ob das Unternehmen eine DSFA durchführen sollte. Andererseits klären, welche technischen und organisatorischen Maßnahmen das Unternehmen implementieren kann, um eine möglichst sichere Verarbeitung zu garantieren (Kapitel 4.4. und 4.6.3.).

Step 5 – Speicherkonzept

Für jede Datenkategorie überlegen, wie lange diese gespeichert werden muss. Danach ein System erarbeiten, um die Löschung nach der notwendigen Zeit sicherzustellen (Kapitel 4.5.).

Step 6 – Verträge mit Dritten

Werden Daten zusammen mit anderen Unternehmen verarbeitet, sollten entsprechende Verträge mit diesen abgeschlossen werden (Auftragsverarbeitungsvertrag, Joint Controller Vertrag, Vereinbarung über die Datenübermittlung) (Kapitel 6.1.4., 6.2.2. und 6.3.).

Step 7 – Verarbeitungsverzeichnis

Das Niederschreiben aller Verarbeitungen ist immer notwendig (Kapitel 4.1.).

Step 8 – Datenschutzerklärung

Vorbereitung der Informationen an betroffene Personen (Kapitel 4.2.).

Step 9 – Anfragebeantwortungskonzept

Überlegen, welche Anfragen am häufigsten gestellt werden könnten, und deren Beantwortung vorbereiten (Kapitel 9.2.).

1.2. Must-haves

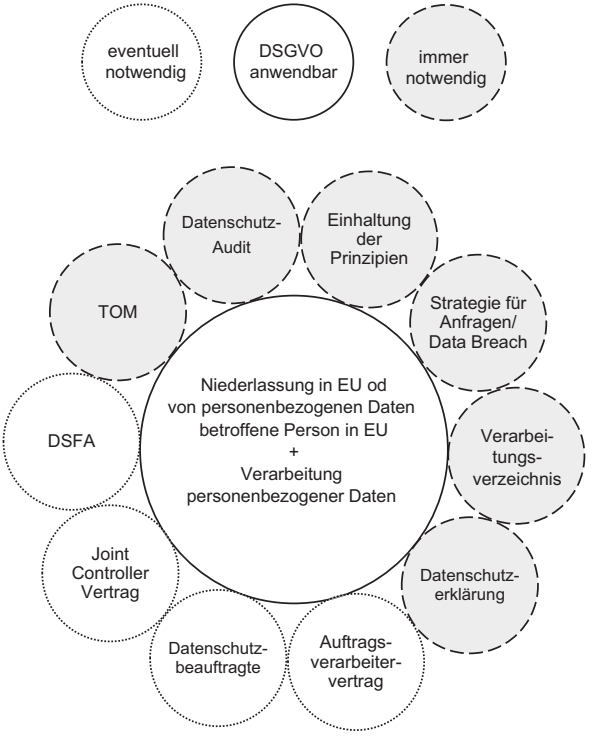

Abb 1: Anforderungen auf einen Blick

1.2.1. Verzeichnis der Verarbeitungstätigkeiten

Verantwortliche und Auftragsverarbeiter müssen gem Art 30 DSGVO selbstverantwortlich Verzeichnisse über ihre Verarbeitungstätigkeiten führen, in denen sie die jeweiligen Datenverarbeitungen genau beschreiben. Das Verzeichnis ist schriftlich zu führen und muss laufend aktualisiert werden. Auf Anfrage der Datenschutzbehörde ist dieser das Verfahrensverzeichnis vorzulegen. In der Praxis sollte bereits vor Aufnahme der Datenverarbeitung eine Risikoeinschätzung sowie eine Prüfung der Rechtmäßigkeit der Datenverarbeitung erfolgen und im Verfahrensverzeichnis dokumentiert werden.

In Kapitel 4.1. ist ein Muster eines Verfahrensverzeichnisses abgedruckt, das die von der DSGVO geforderten Mindestinhalte sowie weitere nützliche Informationen, die in das Verfahrensverzeichnis aufgenommen werden können, enthält.

1.2.2. Datenschutzerklärung

Betroffene Personen haben das Recht, darüber informiert zu werden, was Unternehmen mit ihren personenbezogenen Daten machen.

Der Informationspflicht muss man in einer präzisen, transparenten, verständlichen und leicht zugänglichen Form sowie in einer klaren und einfachen Sprache nachkommen. Eine Datenschutzerklärung ist also ein leicht verständliches Dokument, das Details zur Datenverarbeitung enthält. Die DSGVO sieht Mindestinformationen wie Daten der Verantwortlichen, Verarbeitungszwecke, Rechtsgrundlage, Empfänger oder Speicherdauer vor, es kann aber auch wesentlich ausführlicher sein.

Für bestimmte Fälle gibt es Ausnahmen von (Teilen) der Informationspflicht, so zB, wenn die Informationen einem Berufsgeheimnis unterliegen oder wenn die betroffene Person bereits über die Informationen verfügt. In den allermeisten Fällen werden Start-ups und KMUs aber eine Datenschutzerklärung benötigen.

Nähere Informationen sowie ein Muster einer Datenschutzerklärung sind in Kapitel 4.2. enthalten.

1.2.3. Speicher-/Löschkonzept

Daten dürfen nicht ewig gespeichert werden. Als Grundregel gilt, dass Daten gelöscht werden müssen, sobald sie nicht mehr für den ursprünglichen Zweck gebraucht werden (zB Handy-Betriebssystem für optimierte Anzeige einer Website nach deren Verlassen).

In bestimmten Fällen besteht aber auch darüber hinaus ein Recht, diese Daten weiterzuverarbeiten, manchmal sogar eine Pflicht. Daher ist es durchaus sinnvoll, sich zu überlegen, welche von den verarbeiteten Daten wann gelöscht werden sollen.

Siehe hierzu Kapitel 4.5.

1.2.4. Strategie für Anfragebeantwortung

Die DSGVO beinhaltet einige Betroffenenrechte, zB das Recht auf Auskunft, Datenübertragbarkeit, Löschung oder Berichtigung. Die Beantwortung hat in der Regel unverzüglich zu erfolgen, maximal aber innerhalb eines Monats (mit Möglichkeit zur Verlängerung). Es ist von Vorteil, sich eine Strategie und ein Muster für Anfragebeantwortungen bereitzulegen, damit im Falle einer Nachfrage klar ist, welche Schritte erledigt werden müssen.

Die Erfahrung zeigt, dass an jedes Unternehmen früher oder später datenschutzrechtliche Anfragen gestellt werden – es zahlt sich also aus, hier vorbereitet zu sein! Siehe dazu Kapitel 9., speziell Kapitel 9.2.

1.2.5. Auftragsverarbeitungsvertrag

Beauftragt ein Verantwortlicher einen anderen mit der Verarbeitung personenbezogener Daten, ist der Auftragnehmer Auftragsverarbeiter iSd DSGVO, sofern er keinen Einfluss auf Mittel und Zweck der Datenverarbeitung hat und nur auf Weisung des Verantwortlichen tätig wird. Zwischen Auftragsverarbeiter und Verantwortlichem ist zwingend ein Auftragsverarbeitungsvertrag abzuschließen, der den Gegenstand der Verarbeitung und die gegenseitigen Pflichten regelt.

In Kapitel 6.1.4. ist ein minimalistisches Muster für einen Auftragsverarbeitungsvertrag abgedruckt, das die von der DSGVO geforderten Mindestinhalte enthält.

1.2.6. Datenschutz-Audit

Eine Einhaltung der datenschutzrechtlichen Vorschriften kann grundsätzlich nicht mit einer einmaligen Umsetzung von Maßnahmen erreicht werden. Die meisten Verpflichtungen verlangen eine laufende Kontrolle und Überprüfung, insb betreffend Sicherheitsmaßnahmen, eingesetzte Auftragsverarbeiter, Aktualität der Verarbeitungstätigkeit und Informationspflichten. Eine regelmäßige Durchführung strukturierter Datenschutz-Audits, entweder vom Unternehmen selbst oder durch einen externen Berater, ist daher unerlässlich.

In Kapitel 4.8. ist ein Muster abgedruckt, das die wesentlichsten Prüffragen für ein Datenschutz-Audit enthält.

1.3. No-Gos

1.3.1. Nichtausreichende Einwilligung

Wer die Einwilligung der betroffenen Person als Rechtsgrundlage heranzieht, muss sicherstellen, dass die Einwilligung den Anforderungen entspricht (siehe dazu Kapitel 3.2.1.1. und 3.2.2.1.).

Ist die Einwilligung nicht auf einen Zweck begrenzt, wurde sie missverständlich, nicht freiwillig bzw nicht ausreichend informiert abgegeben, ist sie ungültig und die gesamte Verarbeitung könnte dadurch nicht rechtmäßig sein. Auch die technische Umsetzung, zB aktives Klicken auf einen Button auf einer Website, muss hier bedacht werden.

1.3.2. Mangelnde Sicherheitsmaßnahmen

Als Datenverarbeiter ist man für die Sicherheit der personenbezogenen Daten bzw der Verarbeitungsvorgänge verantwortlich. Die DSGVO gibt hier einige, nicht näher definierte Vorgaben wie zB Datenschutz durch Technikgestaltung oder durch Voreinstellung und fordert, dass entsprechend dem Risiko der Verarbeitung geeignete Sicherheitsmaßnahmen getroffen werden, wie zB Pseudonymisierung von Daten. Oftmals werden diese Sicherheitsmaßnahmen in der Praxis außer Acht gelassen oder nicht regelmäßig auf Wirksamkeit überprüft, was wiederum vermehrt Datenschutzverletzungen zur Folge haben kann. Mangelnde Sicherheitsmaßnahmen erhöhen daher das Risiko einer Geldbuße, aber auch einer Image-Beeinträchtigung, sollten zB Datenleaks publik werden.

In Kapitel 4.6. finden sich nähere Informationen über die Anforderungen an die zu treffenden Sicherheitsmaßnahmen und konkrete Beispiele.

1.3.3. Verspätete Meldung von Datenschutzverletzungen

Eine Datenschutzverletzung, wie zB ein Hackerangriff, ein irrtümlich verschicktes E-Mail oder der Verlust eines Datenträgers, muss binnen 72 Stunden an die Datenschutzbehörde gemeldet werden, sofern ein Risiko für die Rechte und Freiheiten der Betroffenen besteht. Bei einem voraussichtlich hohen Risiko für die Rechte und Freiheiten der Betroffenen ist zudem eine unverzügliche Meldung an die Betroffenen notwendig.

Das Erkennen und die rasche Aufarbeitung von Datenschutzverletzungen ist also wesentlich – eine verspätete Meldung stellt einen Verstoß gegen die DSGVO dar und könnte zu einer Geldbuße führen, selbst wenn hinsichtlich der Datenschutzverletzung an sich kein Verstoß vorliegt.

In Kapitel 4.7. finden sich mehr Informationen und Beispiele, wann eine Meldung an die Datenschutzbehörde bzw an Betroffene notwendig ist und was diese beinhalten muss.

1.3.4. Verhalten gegenüber der Aufsichtsbehörde

Die Aufsichtsbehörde ist grundsätzlich diejenige Instanz, die eine Geldbuße verhängt und auch deren Höhe bestimmt. Bei der Bemessung der Strafe, die grundsätzlich nach objektiven Merkmalen zu erfolgen hat, sind ua auch getroffene Maß-

nahmen zur Schadensminderung und der Umgang mit der Datenschutzbehörde maßgeblich.

Um einen möglichst positiven Verfahrensausgang zu erwirken, sollte daher von Beginn an, also schon bei etwaigen Prüf- oder Beschwerdeverfahren im Vorfeld eines Verwaltungsstrafverfahrens, ein kooperativer Umgang gepflegt und nicht gegen die Behörde agiert werden. Es ist in der Praxis auch ratsam, umgehend juristischen Beistand zu holen, um in der Kommunikation mit der Behörde keine Fehler zu begehen.

Zudem sollte mit Verfahren vor der Datenschutzbehörde möglichst diskret umgegangen und keine große Medienoffensive gestartet werden. Dies kann nicht nur das Image des Unternehmens belasten, sondern auch die Beziehung mit der Datenschutzbehörde strapazieren und potenziell zu einer höheren Strafe führen.

3. Grundsätze der Verarbeitung

Dieses Kapitel gibt einen Überblick über die Prinzipien, denen jede Datenverarbeitung unterliegt, wobei besonderes Augenmerk auf dem Prinzip der Rechtmäßigkeit liegt und die dort verankerten Rechtsgrundlagen näher beleuchtet werden. In diesem Zusammenhang wird außerdem näher auf Profiling und die damit verbundene automatisierte Entscheidungsfindung eingegangen.

3.1. Prinzipien

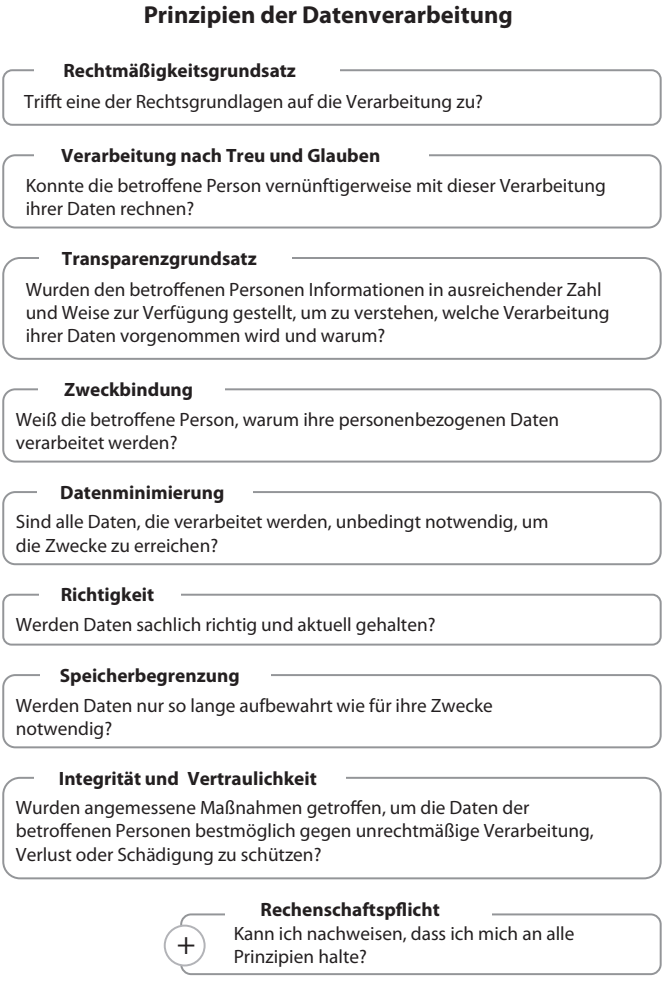

Abb 4: Übersicht Prinzipien

Kurz gesagt

Die in der DSGVO aufgelisteten Prinzipien (siehe Abb oben) stellen das Grundgerüst jeder Verarbeitung dar. Den Prinzipien muss immer entsprochen werden, ihre Verletzung stellt eine grobe Verletzung der Datenschutzregelungen dar. Nur wenn jede der untenstehenden Fragen mit ja beantwortet werden kann, ist die Datenverarbeitung rechtmäßig.

Praxistipp

Prüfen Sie diese Kriterien vor Beginn der Datenverarbeitung genau!

Eine der wichtigsten Bestimmungen der DSGVO findet sich in Art 5. Die dort beschriebenen neun Grundsätze der Verarbeitung bilden die Basis jeglicher Datenverarbeitung und sollten als erste und wichtigste Prüfung der Zulässigkeit der Verarbeitung gesehen werden. Das spiegelt sich auch in den Strafen wider, die bei einer Missachtung dieser Prinzipien oft besonders hoch ausfallen (siehe Kapitel 10.1.1.). Die Prinzipien ziehen sich durch die ganze DSGVO und viele der später beschriebenen Bestimmungen können als Ausformungen oder Präzisierungen dieser Prinzipien gesehen werden.

Im Folgenden findet sich ein Überblick über die Grundsätze sowie jeweils eine Frage, die sich Unternehmen stellen sollten, um einen ersten Eindruck darüber zu erhalten, ob ihre Datenverarbeitung in Einklang mit den Grundsätzen steht. Für eine rechtmäßige Datenverarbeitung müssen alle Grundsätze eingehalten werden.

3.1.1. Rechtmäßigkeitsgrundsatz

Trifft eine der Rechtsgrundlagen auf die Verarbeitung zu?

Jede Verarbeitung muss auf einer der explizit in Art 6 DSGVO (siehe Kapitel 3.2.1.) genannten Rechtsgrundlagen basieren, ansonsten ist die Verarbeitung nicht erlaubt. Werden besondere Kategorien von Daten verarbeitet, muss eine der Ausnahmen gem Art 9 DSGVO (siehe Kapitel 3.2.2.), bei personenbezogenen Daten über strafrechtliche Verurteilungen muss ein Grund gem Art 10 DSGVO zutreffen.

Nicht alle Rechtsgrundlagen und Ausnahmen stellen klare Abgrenzungen dar. Sie bieten somit Argumentationsspielraum für Unternehmen, aber auch ein damit einhergehendes Unsicherheits- und somit Risikopotential.

Beispiel: Rechtsgrundlage

Ein Unternehmen verarbeitet Name, Adresse, Zahlungsdaten und Geschlecht der Kundschaft seines Onlineshops. Eine Einwilligung dieser Personen hierfür wird nicht ein-

geholt. – Während das Unternehmen für die Lieferung und Zahlungsabwicklung (Vertragserfüllung) Name, Adresse und Zahlungsdaten benötigt, gibt es keine Rechtsgrundlage, die die Verarbeitung des Geschlechts rechtfertigt. Sie ist somit nicht erlaubt.

3.1.2. Verarbeitung nach Treu und Glauben

Konnte die betroffene Person vernünftigerweise mit dieser Verarbeitung ihrer Daten rechnen?

Die Verarbeitung muss für betroffene Personen im Rahmen des Erwartbaren, also nicht überraschend, sein. Dazu trägt auch die Art und Weise bei, wie die Daten erhoben werden.[39] Die englische Fassung der DSGVO spricht hier von „Fairness" der Verarbeitung, die Verordnung bleibt leider eine nähere Definition schuldig. Bei Interessenabwägungen sollte immer auf dieses Prinzip geachtet werden.[40]

Beispiel: Treu und Glauben

Eine betroffene Person stellt ein Auskunftsansuchen an ein Unternehmen. Das Unternehmen verarbeitet zwar im Zeitpunkt der Anfrage Daten der betroffenen Person, löscht aber nach der Anfrage alle mit der betroffenen Person zusammenhängenden Daten und schickt eine Negativauskunft. – Eine Löschung der Daten, die nach dem Ersuchen um Auskunft erfolgt, stellt einen Verstoß gegen den Grundsatz von Treu und Glauben dar.[41]

3.1.3. Transparenzgrundsatz

Wurden den betroffenen Personen Informationen in ausreichender Zahl und Weise zur Verfügung gestellt, um zu verstehen, welche Verarbeitung ihrer Daten vorgenommen wird und warum?

Personen müssen **umfassend darüber informiert sein, wie Verantwortliche mit ihren Daten umgehen**: Welche Daten werden verarbeitet, für welche Zwecke, in welchem Ausmaß etc. Neben dem theoretischen Rechtmäßigkeitsgrundsatz steht also dieser praktische Transparenzgedanke. Dieser kommt ganz klar in den Regeln zur Datenschutzinformation und Anfragebeantwortung heraus, er bildet aber auch die Grundlage für die Betroffenenrechte und ist eng mit dem Fairnessgedanken verbunden.

Transparenz ist für jegliche Kommunikation mit den betroffenen Personen zu jedem Zeitpunkt der Verarbeitung essenziell. Wenn es dem Verantwortlichen möglich ist, die Daten den betroffenen Personen direkt über ein sicheres System zur Verfügung zu stellen (zB einen eigenen Punkt dazu im Nutzerprofil), ist das empfehlenswert.[42]

39 ICO, Lawfulness, fairness and transparency, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/ (1.3.2022).
40 *Feiler/Forgó*, EU-DSGVO: Kurzkommentar[1] (2016) Art 5 EU-DSGVO Anm 2.
41 Vgl DSB 27.6.2019, DSB-D124.071/0005-DSB/2019.
42 Vgl ErwGr 63 DSGVO.