

Dr. Heiko Heinrich Stutzke und Wiebke Brüssel
mail@das-strategiebuero.de

August 2021

Download:

Diesen Beitrag können Sie auf unserer Homepage im Bereich „Strategie-Impulse“ als PDF-Datei herunterladen.

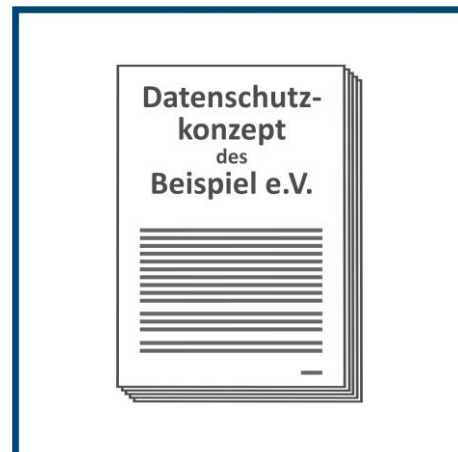
Ein Datenschutzkonzept für soziale (und andere) Organisationen

Die DS-GVO (Datenschutz-Grundverordnung) ist für viele Organisationen im Sozialbereich, aber auch für kleine Firmen und Vereine immer noch eine Herausforderung. Insbesondere beim Thema „Dokumentationen und Nachweispflichten“ gibt es Nachholbedarf. Das hat zwei Ursachen: Zum einen fehlen oft schlicht Informationen zu dieser Materie. Zum anderen ist externe Unterstützung in der Regel so teuer, dass der Aufwand nicht leistbar ist.

Es gibt aber eine Lösung. Doch zunächst werfen wir einen Blick darauf, worum es beim Datenschutzkonzept eigentlich geht.

Die Herausforderung

„Datenschutzkonzept – Muss ich da noch etwas tun?“ Obwohl die DS-GVO bereits im Jahr 2016 eingeführt wurde, stellen sich manche Organisationen, Vereine und kleine Firmen immer noch diese Frage. Das zeigt, wie schwierig die praktische Umsetzung der neuen Anforderungen ist.



Zusammen mit der DS-GVO wurden nicht nur neue Regeln festgelegt, wie personenbezogene Daten von Unternehmen und Organisationen zu behandeln sind. Seitdem gibt es auch zahlreiche Dokumentations- und Nachweispflichten. Während aber über die Regeln (zum Beispiel erforderliche Hinweise auf der Homepage) und den damit verbundenen Aufwand lange und ausführlich in den Medien berichtet wurde, blieb das Thema „Dokumentationen und Nachweise“ meistens am Rande.

Die Folge ist, dass viele Organisationen, Vereine und kleine Firmen nicht wissen, dass die Überarbeitung der Datenschutzerklärung und der Einbau eines entsprechenden Menüpunktes auf der Homepage nur einen kleinen Teil der Aufgaben darstellen, die für die ordnungsgemäße Erfüllung der DS-GVO-Anforderungen zu bearbeiten sind. Hinzu kommt, dass sie aufgrund ihrer

Größe oft keinen eigenen Datenschutzbeauftragten brauchen und das Thema im Tagesgeschäft unterbringen müssen.

Wichtig

Die Nichteinhaltung der Dokumentations- und Nachweispflichten wird von den Aufsichtsbehörden mit hohen Strafen belegt.

Was ist ein Datenschutzkonzept?

Ein Datenschutzkonzept ist eine ausführliche schriftliche Dokumentation. In ihr wird beschrieben, wie ein Unternehmen bzw. eine Organisation mit personenbezogenen Daten arbeitet und wie die Anforderungen der DS-GVO in der täglichen Praxis umgesetzt werden.

Um welche Daten geht es?

Im Datenschutzkonzept geht es um die Daten von Kunden, aber auch von Mitarbeitenden und Kooperationspartnern. Der Schwerpunkt liegt dabei auf den Personenbezogenen Daten.

Personenbezogene Daten sind alle Informationen, die sich auf natürliche Personen beziehen und mit denen eine Person identifiziert werden kann. Hier einige Beispiele für Daten, mit denen eine Person identifiziert werden kann:

- Name,
- Standortdaten,
- Kennnummern (auch Online-Kennungen),
- besondere Merkmale, die spezielle Eigenschaften einer Person beschreiben, zum Beispiel physische, physiologische, genetische, psychische, wirtschaftliche, kulturelle oder soziale Merkmale.

Bestimmte Datenkategorien sind dabei besonders sensibel. Dazu gehören Daten von Kindern, Gesundheitsdaten, ethnische Herkunft, genetische bzw. biometrische Daten, aber zum Beispiel auch Gewerkschaftszugehörigkeit. Werden solche Daten verarbeitet, muss eine Datenschutz-Folgenabschätzung durchgeführt werden. Diese beschreibt, welche Maßnahmen im Falle von Vernichtung, Verlust, Veränderung, unbefugter Offenlegung oder unbefugtem Zugang zu solchen Daten vorgesehen sind, um den entstandenen Schaden zu minimieren.

Wer muss ein Datenschutzkonzept haben?

Die DS-GVO gilt für alle, also für Einzelunternehmer genauso wie für große, international tätige Konzerne. Jede Organisation, jede Firma und jeder Verein, der personenbezogene Daten verarbeitet, muss die Dokumentations- und Nachweispflichten erfüllen. Hierfür bietet sich an, ein schlüssiges Datenschutzkonzept zusammenzustellen.

Warum ist es notwendig, ein Datenschutzkonzept zu haben?

Die DS-GVO selbst fordert die Zusammenstellung eines Datenschutzkonzeptes nur indirekt. Um die DS-GVO zu erfüllen, ergibt sich aber die Notwendigkeit für eine Dokumentation von Verarbeitungsprozessen, organisatorischen Maßnahmen und vielem mehr fast automatisch.

In der Hauptsache geht es um

- die Einhaltung der Verarbeitungsgrundsätze nach Art. 5 DS-GVO und allgemeine Rechenschaftspflichten,
- die Dokumentation und Einholung von Einwilligungen nach Art 7 DS-GVO,
- die Dokumentation der technischen und organisatorischen Maßnahmen (TOM) nach Art. 24 DS-GVO,
- die Dokumentation der Zusammenarbeit mit Auftragsverarbeitern nach Art. 28 DS-GVO,
- die Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 DS-GVO,
- die Behandlung von Datenschutzverletzungen (Art. 33 DS-GVO) und
- eine Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO, soweit erforderlich.

Natürlich kann man jede dieser Anforderungen isoliert betrachten und die entsprechenden Unterlagen zusammenstellen. Deutlich sinnvoller ist es aber, sie im gemeinsamen Kontext und in einem zentralen Dokument zusammenzustellen. Dies erleichtert das Verständnis der komplexen Materie sehr und hilft bei der Klärung von Detailfragen. Weiterhin werden redundante und auseinanderlaufende Informationen vermieden, und Änderungen können leicht an einer einzigen Stelle vorgenommen werden. Auch die Information der Mitarbeitenden wird leichter, und Anforderungen von Aufsichtsbehörden oder Kunden können leichter bearbeitet werden.

Es wird deutlich, dass die Erstellung eines Datenschutzkonzeptes eine Aufgabe ist, die nicht nebenbei erledigt werden kann, sondern mindestens als Projekt mit zugewiesenen Personalressourcen angelegt werden muss, um in vertretbarer Zeit gute Ergebnisse zu bekommen.

Tipp

Führungskräfte und Mitarbeitende, die sich mit der Zusammenstellung des Datenschutzkonzeptes beschäftigen, müssen einen sehr guten Gesamtüberblick über die Aktivitäten des Unternehmens bzw. der Organisation mitbringen und darüber hinaus über ein gutes Verständnis der technischen Umsetzung von Verarbeitungs- und Sicherheitsprozessen verfügen.

Wie ist ein gutes Datenschutzkonzept aufgebaut?

Ein Datenschutzkonzept sollte so aufgebaut werden, dass ein Außenstehender (z.B. eine Behörde) ohne weitere Nachfragen verstehen kann,

- was das Unternehmen bzw. die Organisation macht (der Geschäftszweck),
- wie die wesentlichen Prozesse gestaltet sind, bei denen Daten verarbeitet oder gespeichert werden,
- wie die IT-Struktur aussieht,
- welche Daten wie verarbeitet und gespeichert werden (mit besonderem Augenmerk auf Daten mit einem besonders hohen Vertraulichkeitsgrad),
- wer jeweils verantwortlich für Verarbeitung und Kontrolle ist und
- wie Sicherheitsvorfälle behandelt werden, zum Beispiel Angriffe von Hackern, Einbrüche, Datendiebstahl und ähnliche Vorkommnisse.

Dazu gehört auch, die entsprechenden Rechtsgrundlagen – also die Paragraphen der DS-GVO – als Referenz zu nennen.

Tipp

Das Datenschutzkonzept enthält sehr viele vertrauliche Informationen, die auf keinen Fall Dritten zugänglich gemacht werden dürfen. Die Unterlage muss daher gut gesichert untergebracht werden, zum Beispiel in einem Tresor. Das gilt auch für die Dateien mit den Inhalten. Sie sollten niemals unverschlüsselt per E-Mail versandt oder in nicht ausdrücklich für vertrauliche Informationen geeignete Cloudspeicher eingestellt werden.

Wieviel Zeit muss aufgewendet werden, um das eigene Datenschutzkonzept zu erstellen?

Selbst mit externer Unterstützung dauert die Zusammenstellung eines Datenschutzkonzeptes in der Regel mehrere Monate. Dieser Zeitraum hängt natürlich in weiten Teilen davon ab, wie viel Zeit in Organisation, Verein oder Firma zur Verfügung steht und in welchen Intervallen Abstimmungen erfolgen. Es ist aber völlig normal, wenn die Arbeit am Datenschutzkonzept drei Monate dauert.

Es kommt auch nicht darauf an, möglichst schnell fertig zu sein, sondern ein tragfähiges Konzept zu haben, das dann bei Bedarf durchaus auch für die Planung organisatorischer Veränderungen genutzt werden kann. Es ist also nicht auf den eigentlichen Zweck „DS-GVO und Datenschutz“ beschränkt.

Ein wichtiger Tipp:

Erstellen Sie Ihr Datenschutzkonzept nicht allein, also ohne die Unterstützung eines sachkundigen Beraters. Der notwendige Zeitaufwand wird dann so groß, dass er kaum im normalen Tagesgeschäft untergebracht werden kann, und dann wird die Arbeit immer wieder verschoben.

Ein solches Datenschutzkonzept ist nicht automatisch auch juristisch überprüft; der finanzielle Aufwand für eine solche Prüfung kann jedoch sehr hoch sein. Wenn auf eine juristische Überprüfung verzichtet wird, ist es ausschlaggebend, das Datenschutzkonzept sorgfältig, nach bestem Wissen und Gewissen und ausgerichtet an den Vorschriften der DS-GVO zusammenzustellen.

Wie kann ein guter externer Berater die Arbeit erleichtern?

Firmen, Vereine und andere Organisationen müssen ihr Datenschutzkonzept nur einmal und nur für sich selbst zusammenstellen. Die meisten verfügen dabei nicht über eine umfassende Expertise, was den sinnvollen Aufbau und die inhaltliche Gestaltung betrifft. Diese bringt ein externer Berater mit, der auf die Erfahrungen aus einer Vielzahl entsprechender Projekte zurückgreifen kann.

Im Idealfall stellt Ihnen der Berater ein Textmuster (zum Beispiel als Word-Datei) zur Verfügung, das die Struktur und alle notwendigen Bereiche des Datenschutzkonzeptes in eine sinnvolle Abfolge bringt. Durch vorformulierte Textbausteine können allgemeine Formulierungen direkt übernommen werden, so dass nur diejenigen Informationen eingebaut werden müssen, die Ihre spezifische Organisation betreffen. Hier sollte das Dokument Hinweise enthalten, welche Informationen eingefügt werden müssen.

Wir haben ein solches Dokument für unser eigenes Datenschutzkonzept entwickelt und bieten es auch unseren Kunden an.

Auf diese Weise wird der finanzielle Aufwand für externe Beratung deutlich geringer, da Sie selbst Ihr Fachwissen über Ihre Organisation ins Datenschutzkonzept aufnehmen. Der Berater sollte sie aber bei der Zusammenstellung unterstützen und alle Passagen gemeinsam mit Ihnen durchgehen. So entsteht ein konsistentes Konzept, das den Preisrahmen nicht sprengt.

Im Ergebnis sollte ein Dokument entstehen, das bei Bedarf oder auf Anforderung direkt an anfordernde Stellen (z.B. Landesdatenschutzbeauftragte) gegeben werden kann.

Redaktionelle Hinweise

Über die Autoren

Dr. Heiko Heinrich Stutzke und Wiebke Brüssel sind Geschäftsführende Gesellschafter des Strategiebüros.

Wir moderieren Planungsprozesse - einschließlich Vorbereitung und Dokumentation. Von einer einzelnen Fragestellung bis zur Strategischen Unternehmensplanung. Unsere Kunden sind Unternehmen und Organisationen im privaten, sozialen und öffentlichen Bereich, Firmen am Anfang ihrer Entwicklung und Gründer.

Hinweis zur verwendeten Sprache

Sprachliche Grundlage für unsere Beiträge ist das amtliche Regelwerk des Rates für deutsche Rechtschreibung. Wir sprechen alle Menschen an.

Lobbyregister

Das Strategiebüro ist unter der Kontonummer K4126147 im Lobbyregister des Deutschen Bundestages eingetragen.

Nutzungsrechte

Alle Rechte für unsere Beiträge und die verwendeten Bilder liegen, soweit nicht ausdrücklich anders gekennzeichnet, bei der Das Strategiebüro GbR.

Wir freuen uns, wenn Sie Beiträge und Bilder für Ihre persönliche (ausschließlich private) Information nutzen, sie zitieren oder verlinken. Wenn Sie unsere Beiträge, Bilder oder andere Inhalte jedoch außerhalb der Grenzen des Urheberrechtes ganz oder teilweise für gewerbliche oder öffentliche Zwecke verwenden, in elektronische Medien einstellen oder weitergeben wollen, bitten wir Sie, hierfür unsere schriftliche Genehmigung einzuholen.

