HELBING
Kanzlei für IT- und Datenschutzrecht

ANLEITUNG ZUR MUSTER-DATENSCHUTZRICHTLINIE

VON: Dr. Thomas Helbing, Fachanwalt für IT-Recht

BETREFF: Umsetzung der Muster-Datenschutzrichtlinie (www.thomashelbing.com/dsgvo-sinfonie)

VERSION: 1.1.1

INHALTSÜBERSICHT

Dr. Thomas Helbing
Rechtsanwalt
Fachanwalt für IT-Recht

www.thomashelbing.com

Kopernikusstraße 9
81679 München

T +49 (0) 89 - 45 70 84 05
E helbing@thomashelbing.com

USt.-IdNr. DE815182912

1) GEGENSTAND UND KONZEPTION DER MUSTER-RICHTLINIE

Dieses Dokument erläutert die Nutzung meines Musters für eine „Datenschutzrichtlinie“ („**Muster-Richtlinie**“), abrufbar unter www.thomashelbing.com/dsgvo-sinfonie.

Diese Erläuterung richtet sich an alle, die mit der Umsetzung des Datenschutzrechts im Unternehmen betraut sind, z.B. Datenschutzbeauftragte,

Rechtsanwälte, Berater, Inhouse-Juristen, Geschäftsführer, Inhaber oder Projektleiter.

Die Muster-Richtlinie erklärt den Mitarbeitern Ihres Unternehmens die Anforderungen der Datenschutzgrundverordnung (DSGVO) und legt interne Verantwortlichkeiten und Prozesse zur Umsetzung der DSGVO fest. Sie ist eine Arbeitsanweisung.

Sie können die Muster-Richtlinie grundsätzlich für Unternehmen aller Branchen und Größen nutzen, müssen den Text jedoch an Ihr Unternehmen anpassen. Aufgrund ihres Detailgrads ist die Muster-Richtlinie vor allem gedacht für

- mittelgroße und große Unternehmen, bei denen 100 oder mehr Personen regelmäßig mit personenbezogenen Daten umgehen („White Collar Worker“),
- stark diversifizierte Unternehmen und Unternehmen mit komplexen Strukturen
- Unternehmen mit datengetriebenem Geschäftsmodell
- Unternehmen mit hohen Compliance Anforderungen

Die Muster-Richtlinie beruht auf den Erfahrungen einer Vielzahl von DSGVO-Umsetzungsprojekten und meinen umfassenden Beratungserfahrungen als Rechtsanwalt und externer Datenschutzbeauftragter.

Zur Muster-Richtlinie gehören folgende begleitende Dokumente:

- „Datenschutz-Spickzettel“: Zusammenfassung der wesentlichen Pflichten der Muster-Richtlinie in einfacher Sprache auf zwei Seiten.
- DSGVO Checkliste: Checkliste zur Sicherstellung und Dokumentation der Einhaltung der Datenschutzanforderungen bei einzelnen Verarbeitungstätigkeiten (für Datenschützer, Anwendung erfordert Vorkenntnisse).

Die Muster-Richtlinie erläutert die datenschutzrechtlichen Anforderungen der DSGVO und gibt viele Beispiele (z.B. zu den Informationspflichten und den Anforderungen an Datenschutz-Einwilligung). Ich halte Erläuterungen in einer Datenschutzrichtlinie für geboten: Aufgrund der Komplexität des Datenschutzrechts kann von Mitarbeitern nicht erwartet werden kann, dass sie die Datenschutz-Anforderungen aus Gesetzestexten selbst ableiten oder nach einer Schulung dauerhaft präsent haben. Die Richtlinie dient insofern auch als Nachschlagewerk.

Diese Konzeption bringt es mit sich, dass die Muster-Richtlinie einen gewissen Umfang erreicht. Allerdings sind der Großteil der Bestimmungen der Muster-Richtlinie nur für einen kleinen Teil der Mitarbeiter zu beachten (die „Verarbeitungs-Verantwortlichen“), nur einige Ziffern gelten für alle Mitarbeiter. Die Unterscheidung wird durch die beiden Abschnitte im Datenschutz-Spickzettel sowie Ziffer 3.1 und 3.2 der Muster-Richtlinie deutlich.

Besteht der Wunsch nach einem kürzeren Text können Sie erläuternde Passagen in Anhänge oder gesonderte Dokumente (z.B. One-Pager) auslagern, die z.B. in Ihrem Intranet abrufbar sind.

Am Ende einzelner Abschnitte findet sich ein Link mit „weiterführenden Informationen“ zu einer von mir gepflegten Seite. Dort veröffentliche ich ausgewählte Links zu hilfreichen Quellen. Hierdurch bleibt die Aktualität gewahrt und Mitarbeiter erhalten ergänzende, praxisnahe Hilfestellungen.

Bei der Muster-Richtlinie habe ich darauf geachtet, dass deutlich geregelt ist, wer im Unternehmen konkret welche Verantwortung trägt und Prozessschritte klar festgelegt sind. Hieran mangelt es aus meiner Erfahrung bei Datenschutzrichtlinien häufig. So genügt es etwa nicht, dass auf das Erfordernis von Auftragsverarbeitungsverträgen hingewiesen wird. Vielmehr muss klar sein, wer für den Abschluss der Verträge und die Prüfung der Dienstleister verantwortlich ist. Ansonsten droht ein Zuständigkeitswirrwarr zwischen Fachabteilung, Einkauf, Rechtsabteilung und Datenschutzbeauftragtem.

Die Muster-Richtlinie hat ihren Fokus auf den Datenschutz. Fragen der Datensicherheit werden nur abstrakt behandelt. Es bedarf insofern einer ergänzenden Informationssicherheitsrichtlinie, nach der Informationen (nicht nur personenbezogene Daten) Schutzklassen zugeordnet werden und für jede Schutzklasse konkrete Sicherheitsmaßnahmen festgelegt werden (z.B. sicherer Transport und sichere Löschung).

2) VORTEILE UND NUTZEN EINER DATENSCHUTZRICHTLINIE

Auch wenn Ihr Unternehmen keine oder wenige schriftliche Arbeitsanweisungen nutzt, empfehle ich dies beim Datenschutz aus folgenden Gründen:

- Eine Arbeitsanweisung hilft, ein Organisationsverschulden der Unternehmensführung bzw. seiner Führungskräfte und damit Haftungsrisiken zu vermeiden. Sie ist wesentlicher Bestandteil eines Datenschutz-Management-Systems.
- Ihr Unternehmen muss aufgrund der sogenannten „Rechenschaftspflicht“ nachweisen können, die DSGVO einzuhalten (Art. 24 Abs. 1 DSGVO), zum Beispiel bei einer Prüfung durch eine Aufsichtsbehörde oder sonstigen internen oder externen Kontrollen (Revision, Wirtschaftsprüfer, Datenschutzaudits von Kunden, Lieferanten oder Investoren). Die nachweisbare Festlegung von Verantwortlichkeiten und Prozessen ist ein wesentlicher Baustein zur Einhaltung der Rechenschaftsplicht.
- Mitarbeiter erhalten eine konkrete Anleitung zur Einhaltung der DSGVO. Mit einer Richtlinie können Sie die für den Laien nicht verständlichen gesetzlichen Regelungen vereinfacht und unternehmensbezogen darstellen.
- Sollte eine Datenschutz-Aufsichtsbehörde einen DSGVO-Verstoß feststellen, kann argumentiert werden, dass kein strukturelles Versagen vorliegt, sondern interne Prozesse nur im Einzelfall nicht eingehalten wurden. Dies kann sich bei der Bemessung der Bußgeldhöhe günstig auswirken.
- Die Überwachung der Einhaltung der DSGVO (z.B. durch den Datenschutzbeauftragten oder die Revision) wird erleichtert, da der Ist-Zustand mit einem definierten Soll-Zustand (Datenschutzrichtlinie) verglichen werden kann.

Daneben bieten sich ggf. Anweisungen zur Nutzung der geschäftlichen E-Mail Adresse und des Internetzugangs an (Verbot/Erlaubnis privater Nutzung, Kontrollen), sowie Regelungen zur Nutzung von unternehmenseigener und privater Hardware (z.B. „Bring Your Own Device“). Sinnvoll können zudem spezifische Regeln zum Umgang mit personenbezogenen Daten beim Direktmarketing bzw. Vertrieb sein.

3) NUTZUNGSRECHTE AN DEN DOKUMENTEN

Es gelten meine Lizenzbestimmungen "Kostenlos mit Namensnennung / Kostenpflichtig als White Label" (www.thomashelbing.com/lizenz).

Verkürzt gesagt dürfen Sie die Dokumente kostenlos nutzen (auch geschäftlich als Berater), wenn Sie Logo und Autorenhinweise in der Kopf- und Fußzeile unverändert lassen. Gegen eine einmalige Gebühr können Sie eine „White Label" Lizenz kaufen, das Logo und die Autorenhinweise löschen bzw. ändern.

4) ANPASSUNGS- UND ERGÄNZUNGSBEDARF

Lesen Sie bitte die Muster-Richtlinie zunächst einmal vollständig durch und beginnen Sie erst im Anschluss, die Muster-Richtlinie anzupassen.

Die gelb markierten Passagen der Muster-Richtlinie müssen Sie auf jeden Fall ausfüllen.

Zudem empfehle ich, die kursiv gedruckten Beispiele in der Muster-Richtlinie gegebenenfalls um Unternehmensspezifische Fälle zu ergänzen oder an diese anzupassen, damit sich Mitarbeiter besser „wiederfinden".

Je nach Branche und Unternehmensstruktur können individuelle Ergänzungen nötig sein (z.B. wenn Ihr Unternehmen einen IT-Dienstleister ist, im Pharma- oder Gesundheitsbereich agiert oder die Richtlinie auch für Auslandsstandorte gelten soll).

Die folgenden Themen werden zwar von der Muster-Richtlinie behandelt. Je nach Unternehmensgröße und Compliance-Anforderungen können aber weitere Detailregelungen in Spezialrichtlinien sinnvoll sein:

- Datenschutzorganisation: Bei großen Organisationen, die sich ggf. über mehrere Standorte, Tochtergesellschaften und Länder erstrecken, sollten die in der Muster-Richtlinie vorgesehenen Rollen durch Datenschutzkoordinatoren bzw. Fachbereichs-Kontaktpersonen ergänzt und ggf. die Rolle eines „Konzern-Datenschutzbeauftragten" definiert werden. Hierzu bietet sich eine gesonderte Datenschutz-Organisationsrichtlinie an. Neben der Bestellung, der Abberufung, den Aufgaben und Vertreterregelungen der einzelnen Rollen können Sie dort auch das Datenschutz-Berichtswesen und Datenschutz-Kontrollen regeln.
- Löschen von personenbezogenen Daten: Das Löschen von personenbezogenen Daten ist eine komplexe Aufgabe und erfordert die Erstellung von unternehmensweiten und verarbeitungsspezifischen Löschkonzepten. Dies kann in einer gesonderten Richtlinie geregelt werden (Schritte zum Vorgehen bei der Erstellung eines Löschkonzeptes, einheitliche Löschregeln für bestimmte Datenarten).
- Erfüllung von Betroffenenrechten: Die DSGVO kennt eine Vielzahl von teilweise ähnlichen Betroffenenrechten (z.B. Auskunft, Datenkopie, Datenübertragbarkeit) und stellt Vorgaben für die Form und Frist der Bearbeitung durch das Unternehmen auf. Hierzu können Verantwortlichkeiten und Prozesse detaillierter geregelt werden, um eine sichere und effektive Bearbeitung entsprechender Anfragen sicherzustellen.
- Datenschutzfolgenabschätzung: Bei bestimmten risikoreichen Verarbeitungen müssen Datenschutzfolgenabschätzungen durchgeführt

werden. Dies ist ein relativ komplexer Prozess mit vielen Beteiligten. In einer gesonderten Richtlinie können die einzelnen Schritte und die Verantwortlichkeiten näher festgelegt und Muster bzw. Vorlagen für die Prüfung bereitgestellt werden.

- Umgang mit Datenschutzvorfällen: Datenpannen müssen dokumentiert und in bestimmten Fällen Behörden innerhalb von 72 Stunden gemeldet bzw. Betroffene benachrichtigt werden. Damit im Falle eines Falles alles schnell und geordnet abläuft und jeder Beteiligte weiß, was er zu tun hat, können entsprechende Prozesse in einer Richtlinie noch detaillierter geregelt und Vorlagen bereitgestellt werden.

Wenn Sie anwaltliche Unterstützung bei der Anpassung der Muster-Richtlinie oder dem Entwurf von Spezialrichtlinien benötigen, sprechen Sie mich gerne an.

5) ROLLEN UND VERANTWORTLICHKEITEN

Die Richtlinie unterscheidet fünf Rollen, die jeweils bestimmte Aufgaben übernehmen (siehe Ziffer 3 der Muster-Richtlinie):

- Datenschutz-Manager
- Verarbeitungs-Verantwortlicher
- Datensicherheits-Manager
- Datenschutzbeauftragter
- Mitarbeiter

Für die Rollen „Datensicherheits-Manager“ und „Datenschutz-Manager“ müssen Sie jeweils einen Mitarbeiter in Ihrem Unternehmen benennen und die Kontaktdaten in den Anhang der Muster-Richtlinie eintragen.

a) *Datenschutz-Manager*

Der Datenschutz-Manager übernimmt umfassende Aufgaben bei der Umsetzung der DSGVO-Anforderungen (Prüfung, Dokumentation und Organisation) und muss mit der Richtlinie und der DSGVO gut vertraut sein bzw. vertraut gemacht werden.

- Zuverlässigkeit, Sorgfalt und gute Arbeitsorganisation sind wichtige Voraussetzungen.
- In Frage kommen z.B. Mitarbeiter aus dem Bereich Recht, Compliance oder Datenschutz.
- Der Datenschutzbeauftragte, falls ein solcher benannt ist, kann die Rolle des Datenschutz-Managers an sich nicht übernehmen, da er sich sonst selbst kontrollieren würde und Interessenskonflikten ausgesetzt wäre.
- In der Praxis nimmt der Datenschutzbeauftragte allerdings häufig schon Aufgaben wahr, die nach der Muster-Richtlinie in die Verantwortung des Datenschutz-Managers fallen. Denkbar ist insofern, dass sich der Datenschutz-Manager eng mit dem Datenschutzbeauftragten, einem externen Berater oder einem Inhouse-Juristen abstimmt und von diesem unterstützt wird. Zudem wäre möglich, zumindest einzelne Aufgaben des

Datenschutz-Managers dem Datenschutzbeauftragten zuzuweisen (z.B. Pflege des Verzeichnisses der Verarbeitungstätigkeiten).

b) *Datensicherheits-Manager*

Der Datensicherheits-Manager übernimmt Aufgaben im Bereich IT-Sicherheit (z.B. Prüfung von Sicherheitsmaßnahmen von Dienstleistern, Mitwirkung im Prozess bei Datenschutzfolgenabschätzungen oder Datenpannen).

- Fachwissen zur Datensicherheit ist notwendig.
- In Frage kommen Mitarbeiter aus der IT, Informationssicherheit, nicht jedoch der Datenschutzbeauftragte.
- Findet sich intern kein passender Mitarbeiter, kann ein Mitarbeiter als Datensicherheits-Manager benannt werden, der die Erfüllung durch einen externen Dienstleister koordiniert und sicherstellt. Zudem ist eine enge Zusammenarbeit mit dem Datenschutzbeauftragten möglich.

c) *Verarbeitungs-Verantwortlicher*

Als „Verarbeitungs-Verantwortlicher“ wird in der Muster-Richtlinie derjenige Mitarbeiter bezeichnet, der für einen Prozess, ein Verfahren oder ein Projekt, bei dem personenbezogene Daten verarbeitet werden, fachlich konzeptionell verantwortlich ist (z.B. Leiter Personal ist für Online Bewerberplattform verantwortlich, Leiter Gebäudesicherheit für die Videoüberwachung im Außenbereich).

Der Verarbeitungs-Verantwortliche erhält durch die Muster-Richtlinie verschiedene Aufgaben im Zusammenhang mit „seinen“ Verarbeitungen, z.B. die Dokumentation oder den Abschluss von Datenschutzverträgen mit Dienstleistern.

Der Verarbeitungs-Verantwortliche muss nicht explizit benannt werden, ein Mitarbeiter erlangt durch seine fachliche Verantwortung die zugehörigen Datenschutz-Aufgaben. Er wird dabei durch den Datenschutz-Manager unterstützt. Die Verantwortung liegt damit im Wesentlichen bei den Fachbereichen, diese werden durch eine zentrale „Service-Einheit“, den Datenschutz-Manger unterstützt, der zudem gewisse übergreifende Aufgaben wahrnimmt (z.B. Bereitstellung von Musterverträgen, Koordination, zentrale Dokumentation).

Der „Verarbeitungs-Verantwortliche“ ist ein Mitarbeiter des Unternehmens. Der Begriff dient der internen Verantwortungszuweisung und hat nichts mit dem „Verantwortlichen“ im Sinne von Art. 4 Nr. 7 DSGVO zu tun. Verantwortlicher nach Art. 4 Nr. 7 DSGVO ist immer das Unternehmen als Ganzes.

d) *Datenschutzbeauftragter*

Die Muster-Richtlinie sieht die Rolle des Datenschutzbeauftragten vor, kann aber auch verwendet werden, wenn kein Datenschutzbeauftragter benannt wurde. In letzterem Falle sollte geprüft werden, ob eine gesetzliche Pflicht zur Benennung besteht und falls nicht, ob ein Datenschutzbeauftragter freiwillig benannt werden soll.