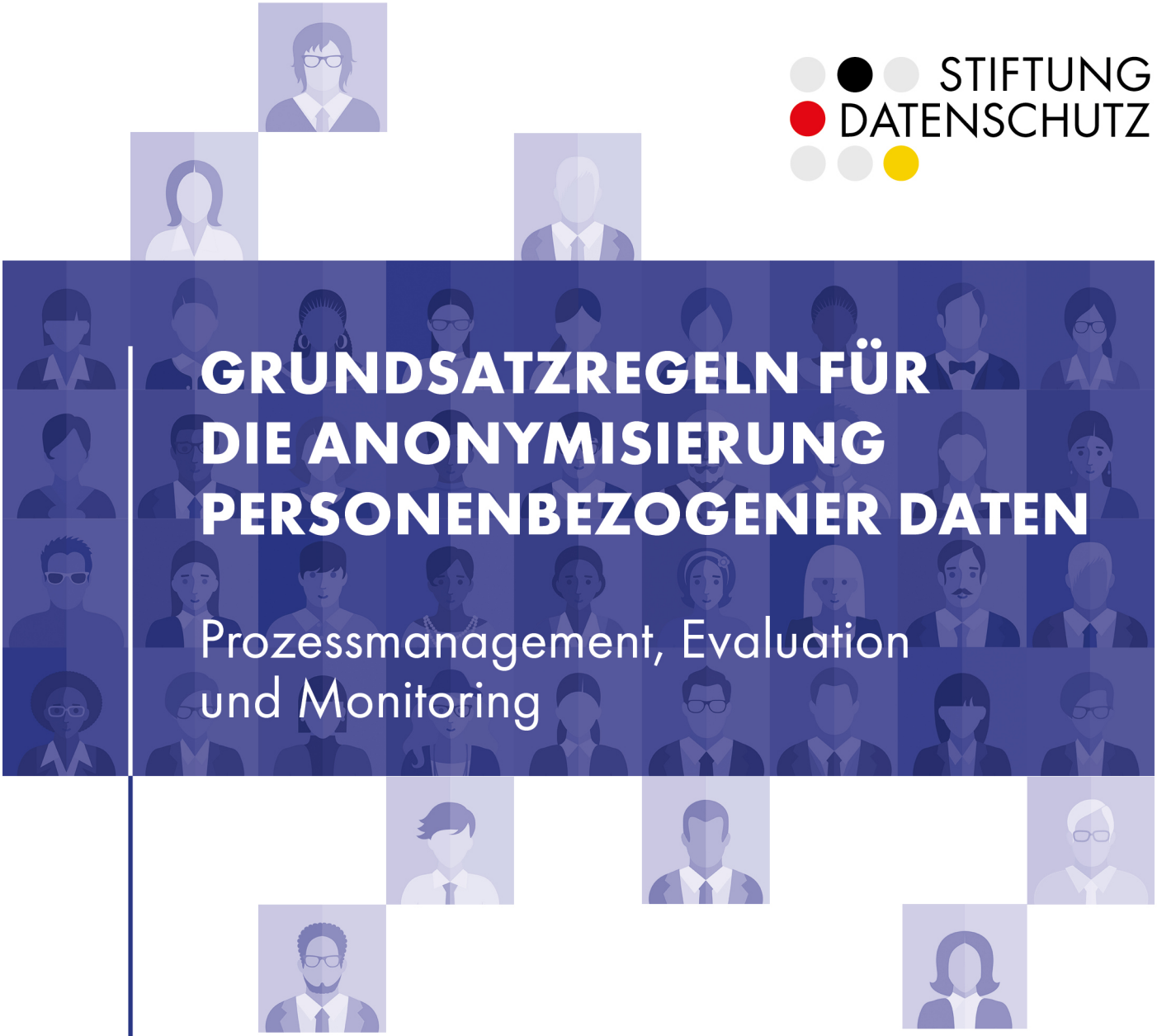

STIFTUNG DATENSCHUTZ

GRUNDSATZREGELN FÜR DIE ANONYMISIERUNG PERSONENBEZOGENER DATEN

Prozessmanagement, Evaluation und Monitoring

VON

Prof. Dr. Rolf Schwartmann, Andreas Jaspers, Dr. Niels Lepperhoff, Steffen Weiß LL.M.

Grundsatzregeln für die Anonymisierung personenbezogener Daten

Prozessmanagement, Evaluation und Monitoring

erstellt und vorgelegt im Auftrag der Stiftung Datenschutz

im Dezember 2022

von

Professor Dr. Rolf Schwartmann
Kölner Forschungsstelle für Medienrecht, Technische Hochschule Köln,
Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.,

Rechtsanwalt Andreas Jaspers
Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.,
DSZ Datenschutz Zertifizierungsgesellschaft mbH,

Dr. Niels Lepperhoff
DSZ Datenschutz Zertifizierungsgesellschaft mbH,
XAMIT Bewertungsgesellschaft mbH,

Rechtsanwalt Steffen Weiß, LL.M.
Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.

Inhaltsverzeichnis

1. Ziel und Ersteller

Die folgenden Grundsatzregeln wurden für die Stiftung Datenschutz erstellt und basieren auf dem „Praxisleitfaden zum Anonymisieren personenbezogener Daten“.[1] Sie sind keine Verhaltensregel gem. Art. 40 DS-GVO, sondern als allgemeingültiger Regelungskatalog gedacht. Verbände oder sonstige Vereinigungen, die Datenverarbeiter vertreten, können allgemeine oder sektorspezifische Verhaltensregeln auf Basis dieser Grundsatzregeln entwickeln, wenn hierbei die Anonymisierung personenbezogener Daten geregelt werden soll. Um als Verhaltensregel genehmigt zu werden, sind ggf. Ergänzungen und Konkretisierungen erforderlich.

2. Allgemeine Begriffsdefinitionen

- **Anonyme Daten** sind Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen.
- **Datensatz:** Die zu einer Person gehörige Information.
- **Direkte Identifikationsmerkmale:** Alle Angaben, welche die Bestimmung einer Person unmittelbar ermöglichen (z.B. Name oder Anschrift).
- **Indirekte Identifikationsmerkmale:** Alle Daten, die nicht zu den direkten Identifikationsmerkmalen gehören, aus denen jedoch ein Personenbezug hergestellt werden kann. Zum Beispiel wenn sie einmalig sind und diese Information mit einer Person in Verbindung gebracht werden kann.
- **K-Anonymität:** Eine Datensammlung bietet k-Anonymität, falls die darin noch enthaltenen Daten jeder einzelnen Person mit mindestens k - 1 anderen Personen übereinstimmen. K ist hier eine natürliche Zahl.
- **Personenbezogene Daten:** Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Nr. 1 DS-GVO).
- **Re-Identifizierung** ist die Bestimmung einer natürlichen Person auf Basis eines anonymisierten Datensatzes.

3. Anwendungsbereich der Grundsatzregeln

Diese Grundsatzregeln gelten für Verantwortliche unabhängig ihrer Branche oder ihres Sektors, wenn sie personenbezogene Daten selbst anonymisieren sowie für Auftragsverarbeiter, die die Anonymisierung personenbezogener Daten im Auftrag von Verantwortlichen durchführen. Die Grundsatzregeln gelten unabhängig von der internen Organisations- und Aufgabenverteilung des Verantwortlichen oder Auftragsverarbeiters. Verantwortliche oder Auftragsverarbeiter, die in ihren Diensten oder Produkten anonymisierte Daten einsetzen, können über diese Grundsatzregeln nachweisen, dass die verwendeten anonymisierten Daten nach den hierin definierten Regeln erstellt wurden und eine Re-Identifikation während der Nutzungsdauer unwahrscheinlich ist. Verantwortliche und Auftragsverarbeiter entscheiden selbst, welche Anonymisierungsprozesse diesen Grundsatzregeln unterworfen werden. Bei denjenigen Produkten,

[1] https://stiftungdatenschutz.org/anonymisierung.

Dienstleistungen oder sonstigen Datenverarbeitungen, die auf anonymisierte Daten zurückgreifen, die nach diesen Grundsatzregeln anonymisiert wurden, ist auf diesen Umstand transparent hinzuweisen.

4. Einzuhaltende Anforderungen

4.1 Organisatorische Maßnahmen

Unbeschadet der sonstigen Pflichten der DS-GVO für Verantwortliche und Auftragsverarbeiter koordiniert der Fachverantwortliche für die Anonymisierung die einzelnen organisatorischen Verantwortlichkeiten vor, während und nach der Durchführung der Anonymisierung.

.

Nummer	Anforderung
1.0	Benennung eines Fachverantwortlichen für die Anonymisierung. ***Hinweis:*** *Das Risiko einer Re-Identifizierung Betroffener ist anhand eines anonymisierten Datensatzes zu beurteilen. Die Prüfung erfordert besondere Kenntnisse im Bereich der Anonymisierungstechniken, der statistischen Verfahren aber auch des Sektors, in dem sich die Anonymisierung bewegt. Daher bedarf es einer fachkundigen Person oder Abteilung, die diese Beurteilung vornimmt.*

4.2 Ermittlung und Dokumentation der zur Festlegung der Anonymisierungsmethode notwendigen Kriterien

Die nachstehenden Anforderungen finden in der konzeptionellen Phase einer Anonymisierung Anwendung. Sie bilden die notwendigen Erwägungen ab, um die Anonymisierung in einem zweiten Schritt (s. Kapitel 4.3) technisch durchzuführen.

Nummer	Anforderung
2.0	Dokumentation der Umstände der Verarbeitung: – Art der verarbeiteten personenbezogenen Daten ***Hinweis:*** *Es sind alle Datenfelder aufzulisten, die anonymisiert werden sollen.* – Beabsichtigte Verarbeitungszwecke ***Hinweis:*** *Die Zwecke sind zu beschreiben, für die die anonymisierten Daten verwendet werden sollen. Es ist zwischen Zwecken des Verantwortlichen und Dritter zu unterscheiden.* – Rechtsgrundlage

Hinweis: *Die Anonymisierung stellt eine Verarbeitung personenbezogener Daten dar, was eine Rechtsgrundlage nach Art. 6 oder 9 DS-GVO erforderlich macht. Der Zweck der Verarbeitung ist bei der Prüfung der Rechtsgrundlage zu würdigen.*

- Kontext der Anonymisierung anhand folgender Parameter:
  - Interne Nutzung anonymisierter Daten oder
  - Weitergabe an bestimmte(n) Empfänger
  - Veröffentlichung

  Hinweis: *Welche Kenntnisse und Fähigkeiten einem Angreifer unterstellt werden, hängt vom Verwendungskontext der anonymisierten Daten ab. Sollen die Daten veröffentlicht werden, ist ein - mit Blick auf die Vielzahl von (kriminellen und staatlichen) Akteuren - von einem tieferen Fachwissen und einer höheren Ausstattung auszugehen, als wenn die Daten an einen bestimmten Empfänger weitergegeben werden.*

- Risiken für Rechte und Freiheiten Betroffener im Falle einer Re-Identifizierung

  Hinweis: *Beschreibung möglicher Risiken für Rechte und Freiheiten Betroffener im Falle eine Re-Identifizierung (z.B. Verlust der Kontrolle über ihre personenbezogenen Daten, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person)**.**

- Erwartete Anzahl an Datensätzen

  Hinweis: *Die Anzahl der zu erwartenden Datensätze ist bei der Anwendung einer oder mehrerer Anonymisierungstechniken von Bedeutung. Eine geringe Anzahl an Datensätzen kann sich bspw. negativ auf eine k-Anonymität auswirken. Je mehr Merkmale vorhanden sind, desto mehr Datensätze werden benötigt.*

- Ermittlung der statistischen Eigenschaften in den Datensätzen, die benötigt werden und welche Merkmale für diese Eigenschaften relevant sind

  Hinweis: *Je nach Zweck der Anonymisierung werden bestimmte statistische Eigenschaften aus einem ursprünglich personenbezogenen Datensatz benötigt. Anonymisierungstechniken verändern die statistischen Eigenschaften des Datensatz mehr oder weniger stark.*

	– Geeignete Anonymisierungsverfahren ***Hinweis:*** *Nach Ermittlung der Umstände der Verarbeitung sind geeignete Anonymisierungsverfahren zu prüfen (zu den verschiedenen Techniken vgl. Praxisleitfaden zur Anonymisierung personenbezogener Daten[2]).* – Festlegung der geeigneten Anonymisierungsmethode(n) und des Zeitpunkts der Anonymisierung ***Hinweis:*** *Aus bestehenden Anonymisierungstechniken sind eine oder mehrere geeignete Methoden auszuwählen. Darüber hinaus ist der Zeitpunkt der Anonymisierung festzulegen, d.h. wann mit der Transformation der personenbezogenen Daten in anonymisierte Daten begonnen wird. Die Dokumentation des Zeitpunktes ist wichtig, um einen Ausgangspunkt für die nachgelagerte regelmäßige Überprüfung der Anonymisierung (s. Kapitel 4.10) zu haben.*

4.3 Durchführung der Anonymisierung

Nummer	Anforderung
3.0	Entfernung aller direkten Identifikationsmerkmale.
3.1	Entfernen aller nicht benötigten indirekten Identifikationsmerkmale.
3.2	Analyse, ob Risiken nach Kapitel 4.9 bestehen.
3.3	Bei bestehenden Risiken nach Nr. 3.2 Durchführung eines oder mehrerer Verfahren der • Randomisierung • Generalisierung oder • solcher mit synthetischen Daten.
3.4	Analyse, ob Risiken zur Re-Identifizierung nach Kapitel 4.9 weiterhin bestehen.
3.5	Sofern Risiken bestehen, Anwendung weiterer Verfahren nach Nr. 3.3.
3.6	Prüfen, ob die benötigten statistischen Eigenschaften erhalten geblieben sind.
3.7	Falls zum Erhalt der statistischen Eigenschaften weiterhin mit Risiken einer Re-Identifizierung zu rechnen ist, ist die weitere Datenverwendung einzustellen.
3.8	Prüfung und Ergebnis dokumentieren.

[2] https://stiftungdatenschutz.org/anonymisierung.

4.4 Weitergabe anonymisierter Daten an Dritte

Im Falle einer Weitergabe anonymisierter Daten an Dritte gelten die nachfolgenden Anforderungen.

4.4.1 Allgemeine Anforderungen

Nummer	Anforderung
4.1	Vereinbarung einer für den Empfänger bindenden Prüfpflicht, ob eine Re-Identifizierung von natürlichen Personen auf Basis der anonymisierten Daten möglich ist.
4.2	Weitergabe nur für die Zwecke des Empfängers notwendiger Daten. ***Hinweis:*** *Je mehr Informationen ein Empfänger erhält, desto höher ist das Risiko einer Re-Identifizierung Betroffener. Deshalb ist der Datensatz auf die Daten zu reduzieren, die der Empfänger objektiv für seine Zweckerreichung benötigt.*

4.4.2 Gemeinsame Verantwortlichkeit

Nummer	Anforderung
5.1	Prüfen, ob eine gemeinsame Verantwortung nach Art. 26 DS-GVO vorliegt.
5.2	Festlegung des für die Durchführung der Anonymisierung zuständigen Verantwortlichen in der Vereinbarung zur gemeinsamen Verantwortlichkeit nach Art. 26 DS-GVO.
5.3	Festlegen, ob und wer für die regelmäßige Überprüfung der Anonymisierung nach Kapitel 4.10 verantwortlich ist.

4.5 Rechte- und Rollenkonzept

Nummer	Anforderung
6.1	Definition von mindestens zwei sich voneinander unterscheidenden Rollen: – (1) Rolle mit Zugriffsberechtigung auf den zu anonymisierenden Datensatz – (2) Rolle mit Zugriff auf die anonymisierten Daten
6.2	Nichtvergabe der Rolle (1) an Empfänger anonymisierter Daten ***Hinweis:*** *Bei den Empfängern sind sowohl interne als auch externe Empfänger zu berücksichtigen.*

4.6 Grundsätze der Verarbeitung personenbezogener Daten

Nummer	Anforderung
7.1	Ermittlung der Rechtsgrundlage für die Anonymisierung.
7.2	Information der Betroffenen im Rahmen der Informationspflichten nach Art. 13 und 14 DS-GVO über die Anonymisierung ihrer personenbezogenen Daten bei Datenerhebung mit folgenden Mindestinhalten: – Vornahme der Anonymisierung – Zweck der Anonymisierung – Einschlägige Rechtsgrundlage

4.7 Unbeabsichtigte/unrechtmäßige Re-Identifizierung von Betroffenen

Nummer	Anforderung
8.1	Dokumentation eines Reaktionsplans für den Fall einer unbeabsichtigten oder unrechtmäßigen Re-Identifizierung von Betroffenen mit den folgenden Mindestinhalten: – Prüfung des Vorliegens einer Rechtsgrundlage für die personenbezogene Datenverarbeitung – Bewertung einer Meldepflicht nach Art. 33 / Art. 34 DS-GVO – Verpflichtende Löschung der personenbezogenen Daten im Falle einer fehlenden Rechtsgrundlage ***Hinweis:*** *Die Erstellung eines eigenen Reaktionsplans ist nicht erforderlich. Der Reaktionsplan kann in einen*

	bestehenden Prozess (z.B. ein allgemeiner Incident-Response-Plan) beim Verantwortlichen oder Auftragsverarbeiter eingebunden werden.

4.8 Dokumentation

Wenn innerhalb dieser Grundsatzregeln die Dokumentation einer oder mehrerer Maßnahmen gefordert wird, gelten die folgenden Anforderungen an die Dokumentation.

Nummer	Anforderung
9.1	Die getroffenen Abwägungen sind für Dritte nachvollziehbar zu begründen. Referenzen auf weitere Dokumentationen (z.B. ein VVT) sind zulässig, soweit sie Aussagen zu den Umständen der Verarbeitung treffen. Die Referenz muss den konkreten Titel, Speicher- oder Ablageort und die Version des referenzierten Dokuments beinhalten. ***Hinweis:*** *Die im jeweiligen Abschnitt zu erstellende Dokumentation erfüllt mehrere Ziele. Die Dokumentation zwingt den Verantwortlichen bzw. den Auftragsverarbeiter, die Vorgaben dieser Grundsatzregeln systematisch zu bearbeiten. Soweit der Fachverantwortliche für die Anonymisierung auf Zuarbeiten anderer Fachverantwortlicher zurückgreift, verfügt er über eine auch für sich stets nachvollziehbare Informationsbasis. Weiterhin ermöglicht diese Dokumentation dem Fachverantwortlichen die ursprünglichen Annahmen regelmäßig zu überprüfen und bei Bedarf anzupassen. Eine solche Evaluation ist insofern erforderlich, als dass die Datenschutz-Grundverordnung eine Anonymisierung nach dem jeweiligen Stand der Technik verlangt bzw. technologische Entwicklungen in die Frage einer hinreichenden Anonymisierung einzubeziehen sind. Im Übrigen ermöglicht die Dokumentation sowohl dem Fachverantwortlichen sowie anderen Überwachungsorganen im Unternehmen (z.B. Compliance oder Internal Audit) Konformitätsprüfungen durchzuführen.*

4.9 Angreifermodell

Nummer	Anforderung
10.1	Dokumentation der Annahmen eines Angreifermodells mit den folgenden Mindestinhalten: – Wissen, Mittel sowie weitere Datenquellen eine Angreifers – Wert der Daten für den Angreifer

	Hinweis: *Wie bereits im Rahmen der Dokumentation der Umstände der Verarbeitung personenbezogener Daten erwähnt, hängen Kenntnisse und Fähigkeiten eines Angreifers vom Verwendungskontext der anonymisierten Daten ab. Sollen die Daten veröffentlicht werden, ist ein - mit Blick auf die Vielzahl von (kriminellen und staatlichen) Akteuren - von einem tieferen Fachwissen und einer höheren Ausstattung auszugehen, als wenn die Daten an einen bestimmten Empfänger weitergegeben werden.*
10.2	Durchführung der Risikobewertung mit folgenden Prüfschritten: – Herausgreifen einer natürlichen Person – Verknüpfung von Datensätzen – Ableitung von Merkmalen (Inferenz)
10.3	Werden anonymisierte Daten zum Traineren von Algorithmen verwendet, ist das Angreifermodell auch auf den trainierten Algorithmus anzuwenden. Es ist zu prüfen, ob das vom Algorithmus berechnete Ergebnis zu einer Re-Identifikation führen kann.

4.10 Regelmäßige Überprüfung

Nummer	Anforderung
11.1	Dokumentation des Prüfintervalls basierend auf einer Risikobewertung, welchen Schaden eine Re-Identifizierung für die betroffenen Personen bedeuten könnte.
11.2	Durchführung und Dokumentation im Rahmen des Prüfintervalls, ob Risiken für die Re-Identifizierung natürlicher Personen im anonymisierten Datensatz bestehen. Zu berücksichtigen sind: – Umstände der Verarbeitung nach Kapitel 4.2 – Vorhandene Mittel beim Verantwortlichen oder Auftragsverarbeiter (rechtliche, technische und organisatorische) – Allgemein verfügbare Technologie nach Stand der Technik – Allgemeine technologische Entwicklungen – Das Angreifermodell nach Kapitel 4.9.

5. Überwachung durch die Überwachungsstelle

Gemäß Art. 40 Abs. 4 DS-GVO sind Verfahren vorzusehen, die es einer Überwachungsstelle ermöglichen, zu überwachen, dass die Bestimmungen der Grundsatzregeln eingehalten werden.

5.1 Mitwirkungspflichten

Die Mitwirkung schließt insbesondere ein, dass

1. rechtzeitig die angeforderten Unterlagen und Nachweisdokumente bereitgestellt werden,
2. rechtzeitig erforderliche Angaben gemacht werden,
3. ein uneingeschränktes Zutrittsrecht für Mitarbeiter und Beauftragte der Überwachungsstelle zu den Räumlichkeiten des selbstverpflichteten Unternehmens, soweit mit der Anonymisierung, befasst auch dessen Auftragsverarbeiters und allen weiteren Unterauftragsverarbeitern, sowie allen sonstigen Orten, an denen Daten zur Anonymisierung verarbeitet werden oder von diese Daten zugegriffen wird, besteht und
4. Mitarbeiter und Beauftragte der Überwachungsstelle Zugang zu allen für die Anonymisierung relevanten personenbezogenen Daten und Informationen, Datenverarbeitungsanlagen und -geräten oder Verarbeitungsvorgängen im Zusammenhang mit diesen Grundsatzregeln haben.

Das selbstverpflichtete Unternehmen verpflichtet sich, den Anordnungen der Überwachungsstelle im Rahmen ihrer Aufgaben gemäß Art. 41 DS-GVO, im Rahmen der vertraglichen Vereinbarungen sowie im Rahmen der in diesen Grundsatzregeln niedergelegten Befugnisse Folge zu leisten.

5.2 Mitwirkungspflichten von weiteren Verantwortlichen und Auftragsverarbeitern

Das selbstverpflichtete Unternehmen stellt durch vertragliche Einzelvereinbarung sicher, dass (weitere) Auftragsverarbeiter und weitere, mit dem selbstverpflichteten Unternehmen gemeinsam für die Verarbeitung Verantwortliche denselben Verpflichtungen zur Mitwirkung bei und Duldung von Kontrollhandlungen der Überwachungsstelle unterliegen wie es selbst. Vorstehendes gilt nur, sofern diese Stellen an der Anonymisierung oder der Kontrolle auf Re-Identifikation mitwirken.

5.3 Befugnisse der Überwachungsstelle

Das selbstverpflichtete Unternehmen unterstützt die Überwachungsstelle uneingeschränkt. Es erkennt die folgenden Befugnisse der Überwachungsstelle uneingeschränkt an, denen es sich unterwirft:

1. Prüfung, ob die Voraussetzungen zur Teilnahme, wie in diesen Grundsatzregeln sowie im Antrag beschrieben, und an der Selbstverpflichtung auf diese Grundsatzregeln erfüllt sind,
2. Annahme oder Ablehnung der Teilnahme an der Selbstverpflichtung auf diese Grundsatzregeln,
3. bei Anhaltspunkten für eine vermutete Verletzung der Grundsatzregeln die betroffenen Unternehmen/Auftragsverarbeiter zur Abgabe einer Stellungnahme aufzufordern,
4. die Teilnahme an der Grundsatzregeln befristet auszusetzen,
5. das Unternehmen/den Auftragsverarbeiter von der Teilnahme an den Grundsatzregeln auszuschließen,
6. Kontrollen vor Ort durchzuführen oder durchführen zu lassen,
7. Nachweisdokumente insbesondere in Form von vorzulegenden Musterverträgen, Prozessbeschreibungen u.a. über die Einhaltung der Grundsatzregeln anzufordern,
8. die Datenschutzaufsichtsbehörde über den Ausschluss von den Grundsatzregeln zu informieren,
9. die Teilnahme an der Grundsatzregeln zu veröffentlichen,
10. angemessene Fristen zur Reaktion sowie Behebung zu setzen,
11. sich unmittelbar an die Unternehmensleitung verpflichteter Unternehmen/Auftragsverarbeiter zu wenden,
12. sich im Falle einer Unternehmensgruppe an die höchste Managementebene zu wenden.

5.3.1 Prozess: Kontrolle der Selbstverpflichtung

Die Kontrolle der verpflichteten Unternehmen durch die Überwachungsstelle erfolgt wie nachstehend:

Nr.	Überwachungsstelle	Unternehmen
1	2x jährlich: mind. 5% der Unternehmen zufällig auswählen; davon unabhängig ist mindestens ein Unternehmen jährlich auszuwählen; Mindestabstand zwischen diesen anlasslosen Prüfungen beim gleichen Unternehmen: 2 Jahre. Die erste anlasslose Prüfung erfolgt frühestens 2 Jahre nach der im Rahmen der Antragstellung erfolgten Eingangsprüfung. Eine Pflichtprüfung erfolgt spätestens nach 7 Jahren.	

	Wenn lediglich ein oder zwei Unternehmen den Grundsatzregeln beigetreten sind, werden diese alle 2 Jahre kontrolliert. Zusätzlich werden für die Kontrolle Unternehmen, die innerhalb der letzten 12 Monate vorübergehend suspendiert wurden, ausgewählt, auch wenn die letzte Kontrolle weniger als 2 Jahre zurück liegt.	
2	Geeignete Nachweisdokumente der Befolgung einfordern (z.B. Musterverträge, Prozessbeschreibungen u.a.).	
3		Zusendung der angeforderten Nachweise innerhalb von 4 Wochen.
4	Falls keine oder nicht alle angeforderten Nachweise vorgelegt werden, fehlende Nachweise anmahnen mit Fristsetzung von 2 Wochen.	
5		Fehlende Nachweise innerhalb von 2 Wochen zusenden.
6	Prüfen, ob Nachweise die Befolgung belegen.	
7	Falls nein, weiter bei Nr. 10.	
8	Falls ja, Ergebnis dokumentieren und Unternehmen/Auftragsverarbeiter informieren.	
9	Prozess Ende.	
10	Start Prozess "Sanktionen bei Verletzung der Selbstverpflichtung".	

5.3.2 Prozess: Sanktionen bei Verletzung der Selbstverpflichtung

Nr.	Überwachungsstelle	Unternehmen
1	Beschreibung der Verletzung und Beantwortung der Fragen: – Was wurde getan? – Was hätte laut den Grundsatzregeln getan werden sollen?	
2	Prüfen, ob die Meldepflicht nach Art. 33 DS-GVO ausgelöst werden könnte.	
3	Falls offensichtlich nein, weiter mit 7.	
4	Falls ja, Kopie der Meldung an betroffene Auftraggeber (soweit einschlägig) oder die zuständige	

	Datenschutzaufsichtsbehörde vom verpflichteten Unternehmen anfordern.	
5		Kopie der Meldung an betroffene Auftraggeber (soweit einschlägig) oder die zuständige Datenschutzaufsichtsbehörde unverzüglich, spätestens innerhalb von 7 Tagen, zusenden.
6	Trifft die Kopie oder Begründung der Nichtmeldung nicht innerhalb von 7 Tagen ein, weiter mit 14.	
7	Aufforderung zum unverzüglichen Abstellen der Verletzung bzw. Bestätigung, dass keine Verletzung vorliegt innerhalb von zwei Wochen.	
8		Unverzügliches Abstellen und entsprechende Nachweise innerhalb von 2 Wochen an die Überwachungsstelle senden. Alternativ: Innerhalb von 2 Wochen darlegen, warum keine Verletzung vorliegt.
9	Wenn die Frist verstreicht, weiter mit Schritt 14.	
10	Nachweise der Nachbesserung oder Argumentation, warum keine Verletzung vorliegt, prüfen. Bei schwerwiegenden Verletzungen oder wenn die Nachbesserung nicht oder nicht effektiv ohne eine Kontrolle vor Ort oder anhand von anzufordernden Unterlagen und Auskünften festgestellt oder bewertet werden kann, kann eine Kontrolle vor Ort erfolgen oder können weitere Unterlagen und Auskünfte angefordert werden.	
11	Wenn Nachbesserung nicht ausreichend ist, weiter mit 14.	
12	Mitteilung an Unternehmen, dass Behebung zufriedenstellend ist und Verfahren beendet ist. Zusätzlich wenn Beschwerden den Prozess auslösten: Mitteilung an den Beschwerdeführer über Behebung der Verletzung dieser Grundsatzregeln. Interne Dokumentation der Mitteilung an Unternehmen und Beschwerdeführer.	

13	Prozess Ende.	
14	Wenn zweite Fristsetzung nicht erfolgreich war, weiter mit Schritt 17. Wenn dritte Fristsetzung nicht erfolgreich war, weiter mit Schritt 21.	
15	Wenn Unternehmen nicht nachbessert oder bereits einen erfolglosen Nachbesserungsversuch unternommen hat oder die Kopie der Meldung / Begründung der Nichtmeldung (Nr. 4) nicht rechtzeitig zusendet, Setzung einer 2. Frist zur Erfüllung der ausstehenden Reaktion bzw. Nachbesserung von 14 Tagen.	
16		Reaktion bzw. erfolgreiche Nachbesserung und Nachweis derselben innerhalb von 14 Tagen an Überwachungsstelle senden.
17	Wenn das Unternehmen angemessen reagiert, dann – nach Zusendung der Kopie der Meldung weiter mit Schritt 7, – nach Abstellen der Verletzung oder Darlegung durch das Unternehmen, warum keine Verletzung vorliegt, weiter mit Schritt 10.	
18	Wenn das Unternehmen nicht angemessen reagiert, dann letzte Frist von 3 Tagen setzen.	
19		Reaktion bzw. erfolgreiche Nachbesserung und Nachweis derselbigen innerhalb von 3 Tagen an Überwachungsstelle senden.
20	Wenn das Unternehmen angemessen reagiert, dann – nach Zusendung der Kopie der Meldung weiter mit Schritt 7, – nach Abstellen der Verletzung oder Darlegung durch das Unternehmen, warum keine Verletzung vorliegt, weiter mit Schritt 10.	
21	Start Prozess "Information der Aufsichtsbehörde bei Entzug Selbstverpflichtung"	
22	Ausschluss von der Selbstverpflichtung bis zum Abstellen der Verletzung	

	plus Verbot mit Selbstverpflichtung zu werben. Information des Unternehmens darüber. Information des Beschwerdeführers, sofern vorhanden.	
23	Start Prozess "Veröffentlichung verpflichteter Unternehmen"	
24		Hinweis auf die Selbstverpflichtung aus allen Werbemitteln und anderen Materialien innerhalb von 4 Wochen entfernen.

Das Unternehmen ist berechtigt, einmalig eine Verlängerung der in Schritt 8 genannten Frist auf 8 Wochen begründet zu beantragen. Die Überwachungsstelle entscheidet in eigenem Ermessen, ob die Fristverlängerung gewährt wird. Falls ja, gilt für Schritt 9 die verlängerte Frist.

Die Entscheidung, welche Konsequenzen aus einer Verletzung zu ziehen sind, liegt im Ermessen der Überwachungsstelle. Die Überwachungsstelle trifft im eigenen Ermessen Entscheidungen zum Aussetzen oder den Entzug der Selbstverpflichtung. Der (temporäre) Entzug einer Selbstverpflichtung während der Vertragslaufzeit beendet weder das Vertragsverhältnis noch befreit er von den im Vertrag vereinbarten Pflichten.

5.4 Prozess: Überprüfung auf Verletzung der Selbstverpflichtung bei Beschwerde

Nr.	Überwachungsstelle	Unternehmen
1	Prüfung, ob die Beschwerde nachprüfbare Sachverhalte schildert und die Verletzungshandlung benennt ("substantielle" Beschwerde)	
2	Prüfung, ob sachlicher Anwendungsbereich der Grundsatzregeln von der Beschwerde betroffen ist	
3	Wenn sachlicher Anwendungsbereich nicht betroffen ist, Information des Beschwerdeführers mit Begründung; Prozess Ende	
4	Wenn Beschwerde nicht substanziell ist, Bitte an Beschwerdeführer zur genaueren Darlegung des Sachverhalts oder Beibringung von Belegen des Fehlverhaltens	

5	Wenn der sachliche Anwendungsbereich berührt ist und die Beschwerde substanziell ist, Unternehmen zur Stellungnahme innerhalb von 4 Wochen auffordern. Bei dem Verdacht auf schwerwiegende Verstöße oder in Fällen, wo Anhaltspunkte vorliegen, dass Nachweise für Verstöße beabsichtigt oder unbeabsichtigt vernichtet werden können, findet zusätzlich eine kurzfristige Kontrolle vor Ort statt. Bei offensichtlichem Verstoß gegen diese Grundsatzregeln kann zusätzlich eine zeitweise Anordnung zum Abstellen der Verletzungshandlung erlassen werden.	
6		Innerhalb von 2 Wochen zur Beschwerde Stellung nehmen unter Darlegung, warum die Beschwerde unzutreffend sei oder welche Maßnahmen ergriffen wurden, um die Verletzungshandlung abzustellen.
7	Wenn die Frist ohne Antwort verstreicht, Erinnerung mit Fristsetzung von 2 Wochen versenden.	
8		Innerhalb von 2 Wochen zur Beschwerde Stellung nehmen unter Darlegung, warum die Beschwerde unzutreffend sei oder welche Maßnahmen ergriffen wurden, um die Verletzungshandlung abzustellen.
9	Wenn das Unternehmen antwortet oder die Nachfrist verstrichen ist, Sachverhalt unter Berücksichtigung der vorliegenden Erklärungen des Beschwerdeführers und des Unternehmens sowie der eigenen Erkenntnisse prüfen.	
10	Beim Vorwurf einer schwerwiegenden Verletzung oder wenn der Vorwurf nicht oder nicht effektiv ohne eine Kontrolle vor Ort oder anhand von anzufordernden Unterlagen und Auskünften	

	bewertet werden kann, kann eine Kontrolle vor Ort erfolgen oder können Unterlagen und Auskünfte angefordert werden.	
11	Stellungnahme des Unternehmens belegt Einhaltung und ggf. durchgeführte Vor-Ort-Kontrolle zeigte keine weiteren Mängel: – Beschwerdeführer informieren – Prozess Ende	
12	Stellungnahme des Unternehmens oder ggf. durchgeführte Vor-Ort-Kontrolle zeigt Mängel: Start Prozess "Sanktionen bei Verletzung der Selbstverpflichtung".	

5.5 Prozess: Information der Aufsichtsbehörde bei Entzug der Selbstverpflichtung

Nr.	Überwachungsstelle	Unternehmen
1	Erstellung und Versand eines Schreibens mit Erläuterung der Maßnahme und Begründung.	
2	Ablage des Schreibens	

5.6 Prozess: Veröffentlichung verpflichteter Unternehmen

Nr.	Überwachungsstelle	Unternehmen
1	Aufnahme bei erteilter Selbstverpflichtung in das öffentliche Verzeichnis, zugänglich über die Website der Überwachungsstelle	

5.7 Prozess: Veröffentlichung suspendierter oder entzogener Selbstverpflichtungen

Nr.	Überwachungsstelle	Unternehmen
1	Bei temporärer oder dauerhafter Suspendierung am Eintrag einen Hinweis anbringen, dass die Selbstverpflichtung befristet oder dauerhaft suspendiert wurde	

6. Prozess: Überprüfung der Grundsatzregeln

Nr.	Inhaber der Grundsatzregeln
1	Die Grundsatzregeln unterliegen einer kontinuierlichen Überwachung im Hinblick auf Aktualität und Rechtskonformität. Dies obliegt dem Inhaber der Grundsatzregeln. Der Inhaber legt der zuständigen Aufsichtsbehörde alle drei Jahre einen schriftlichen Bericht insbesondere über Entwicklung der Verbreitung, Sanktionen, Beschwerden sowie etwaige Anpassungsbedarfe der Grundsatzregeln vor. Änderungen und Erweiterungen dieser Grundsatzregeln sind nur nach Genehmigung durch die zuständige Aufsichtsbehörde wirksam.

STIFTUNG
DATENSCHUTZ

Stiftung Datenschutz
rechtsfähige Stiftung bürgerlichen Rechts
Karl-Rothe-Straße 10–14
04105 Leipzig
Deutschland

Telefon 0341 / 5861 555-0
mail@stiftungdatenschutz.org
www.stiftungdatenschutz.org

gestiftet von der Bundesrepublik Deutschland
vertreten durch den Vorstand Frederick Richter

Die Arbeit der Stiftung Datenschutz wird aus dem Bundeshaushalt gefördert (Einzelplan des BMJ).

Bundesministerium der Justiz