# Kurzpapier Nr. 19

# Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DS-GVO

*Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen - möglicherweise abweichenden - Auslegung des Europäischen Datenschutzausschusses.*

## Was regelt die Datenschutz-Grundverordnung (DS-GVO)?

Nach Art. 29 DS-GVO dürfen Beschäftigte eines Verantwortlichen (eines Unternehmens, eines Vereins, eines Verbands, eines Selbstständigen, einer Behörde usw.) oder eines Auftragsverarbeiters personenbezogene Daten ausschließlich auf Weisung des Verantwortlichen oder Auftragsverarbeiters verarbeiten, es sei denn, eine gesetzliche Regelung schreibt eine Verarbeitung dieser Daten vor.

Ergänzend dazu regelt Art. 32 Abs. 4 DS-GVO, dass der Verantwortliche oder Auftragsverarbeiter Schritte unternehmen muss, um sicherzustellen, dass ihm unterstellte Personen (insbesondere seine Beschäftigten), die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen oder Auftragsverarbeiters verarbeiten (es sei denn, eine gesetzliche Regelung schreibt eine Verarbeitung dieser Daten vor). Für den Fall der Auftragsverarbeitung bestimmt Art. 28 Abs. 3 Satz 2 lit. b DS-GVO, dass der Auftragsverarbeiter gewährleisten muss, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben (soweit sie nicht einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen; Letzteres gilt z. B. für privatärztliche, steuerberaterliche oder anwaltliche Verrechnungsstellen).

Selbst wenn nach dem Wortlaut der DS-GVO nur die Beschäftigten eines Auftragsverarbeiters zu „verpflichten“ sind, trifft inhaltlich diese „verpflichtende Unterrichtung“ (im Folgenden: Verpflichtung) auch die Verantwortlichen und ihre Beschäftigten. Wie Verantwortliche diese gesetzliche Verpflichtung umsetzen (und ggfls. der Aufsichtsbehörde nachweisen), ist nicht verbindlich geregelt. Es wird empfohlen, dies in Form einer schriftlichen oder elektronischen Verpflichtungserklärung umzusetzen. Ein Muster für eine solche Verpflichtung finden Sie in der Anlage.

## Zu was soll verpflichtet werden?

Die Verpflichtung von Beschäftigten zur Wahrung des Datengeheimnisses und zur Beachtung der datenschutzrechtlichen Anforderungen ist ein wichtiger Bestandteil der Maßnahmen, die erforderlich sind, damit ein Verantwortlicher (siehe Art. 5 Abs. 2 und Art. 24 Abs. 1 DS-GVO) oder ein Auftragsverarbeiter (siehe Art. 28 Abs. 3 Satz 2 lit. b DS-GVO) die Einhaltung der Grundsätze der DS-GVO sicherstellen und nachweisen kann („Rechenschaftspflicht“). Diese Grundsätze der DS-GVO, festgelegt in Art. 5 Abs. 1 DS-GVO, beinhalten im Wesentlichen folgende Pflichten:

Personenbezogene Daten müssen

a) auf rechtmäßige und faire Weise, und in einer für die betroffene Person nachvollziehbaren

Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);

b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“);

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist („Speicherbegrenzung“);

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).

Kernelement der Maßnahme ist, dass die Beschäftigten auf die Einhaltung betrieblicher Weisungen verpflichtet werden. Die Form der jeweiligen Weisung ist dabei nachrangig. In Frage kommen neben Einzelanweisungen der Vorgesetzten insbesondere Betriebsvereinbarungen und allgemeine Dienstanweisungen. Außerdem kann Prozessbeschreibungen (z.B. aus dem Qualitätsmanagement), Ablaufplänen sowie Dokumentationen (z.B. Verzeichnis von Verarbeitungstätigkeiten) und Handbüchern Weisungscharakter zukommen.

## Wer muss verpflichtet werden?

Der Kreis der zu verpflichtenden Personen (die DS-GVO spricht insoweit von „unterstellten natürlichen Personen“) ist aufgrund der Bedeutung dieser Regelung weit auszulegen. Insbesondere sind ergänzend zum regulären Mitarbeiterstamm auch Auszubildende, Praktikanten, Referendare, Leiharbeiter und ehrenamtlich Tätige mit einzubeziehen.

Soweit die Verschwiegenheit von Beschäftigten im öffentlichen Bereich gesetzlich oder tariflich ausdrücklich geregelt ist, muss eine solche Verpflichtung nicht erfolgen.

## Wann muss die Verpflichtung erfolgen?

Die Verpflichtung muss bei der Aufnahme der Tätigkeit erfolgen. Sie sollte daher möglichst (spätestens) am ersten Arbeitstag vorgenommen werden.

## Wie muss eine Verpflichtung erfolgen?

Zuständig für die Verpflichtung ist die Unternehmensleitung, der Inhaber einer Firma oder ein von diesen Beauftragter. Selbst wenn, wie oben ausgeführt, die DS-GVO keine bestimmte Form der Verpflichtung vorschreibt, sollte schon aus Nachweisgründen ein spezielles Formular verwendet werden, wobei die Verpflichtung schriftlich oder in einem elektronischen Format erfolgen kann.

Zur Verpflichtung gehört auch eine Belehrung über die sich ergebenden Pflichten. Die Beschäftigten sind - möglichst anhand typischer Fälle - darüber zu informieren, was sie in datenschutzrechtlicher Hinsicht bei ihrer täglichen Arbeit beachten müssen. Mit der Verpflichtung nach der DS-GVO können auch andere Geheimhaltungsvereinbarungen kombiniert werden, z. B. zum Betriebs-, Telekommunikations- oder Steuergeheimnis. Aus Nachweisgründen im Rahmen der Rechenschaftspflicht nach der DS-GVO ist es wichtig, die Verpflichtung ausreichend zu dokumentieren.

## Reicht die einmalige datenschutzrechtliche Verpflichtung?

Zur laufenden Sensibilisierung der Beschäftigten für Fragen des Datenschutzes empfiehlt es sich, in regelmäßigen Zeitintervallen im Rahmen von Schulungen oder in schriftlichen Hinweisen, z. B. in der Betriebszeitung, daran zu erinnern, dass die Beschäftigten verpflichtet worden sind und welche Bedeutung dieser Verpflichtung zukommt. Wenn ein Arbeitsplatzwechsel im Unternehmen oder in der Behörde erfolgt, der mit einem Aufgabenwechsel verbunden ist, sollte dies immer auch zum Anlass genommen werden, die Verpflichtung zu überprüfen und ggf. anzupassen.

***Anlage/Musterbeispiel für eine schriftliche Verpflichtung[1]:***

## Verpflichtung zur Vertraulichkeit und zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung (DS-GVO)

Frau/Herr

verpflichtet sich, personenbezogene Daten nicht unbefugt zu verarbeiten. Personenbezogene Daten dürfen daher nur verarbeitet werden, wenn eine Einwilligung vorliegt oder eine gesetzliche Regelung die Verarbeitung erlaubt oder vorschreibt. Die Grundsätze der DS-GVO für die Verarbeitung personenbezogener Daten sind zu wahren; sie sind in Art. 5 Abs. 1 DS-GVO festgelegt und beinhalten im Wesentlichen folgende Verpflichtungen[2]:

Personenbezogene Daten müssen

a) auf rechtmäßige und faire Weise, und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);

b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“);

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist („Speicherbegrenzung“);

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).

Personenbezogene Daten dürfen daher nur nach Weisung des Verantwortlichen verarbeitet werden. Neben Einzelweisungen der Vorgesetzten gelten als Weisung: Prozessbeschreibungen, Ablaufpläne, Betriebsvereinbarungen, allgemeine Dienstanweisungen sowie betriebliche Dokumentationen und Handbücher[3].

Verstöße gegen diese Verpflichtung können mit Geldbuße und/oder Freiheitsstrafe geahndet werden. Ein Verstoß kann zugleich eine Verletzung von arbeitsvertraglichen Pflichten oder spezieller Geheimhaltungspflichten darstellen. Auch (zivilrechtliche) Schadenersatzansprüche können sich aus schuldhaften Verstößen gegen diese Verpflichtung ergeben. Ihre sich aus dem Arbeits- bzw. Dienstvertrag oder gesonderten Vereinbarungen erge-

[1] Soweit die Verschwiegenheit von Beschäftigten im öffentlichen Bereich gesetzlich oder tariflich ausdrücklich geregelt ist, muss eine solche Verpflichtung nicht erfolgen.
[2] Der Inhalt der Verpflichtung ist im Einzelfall anzupassen. So können bestimmte Aufgaben und Tätigkeiten zusätzliche Unterrichtungen erfordern, etwa zum Beschäftigten- oder Sozialdatenschutz, zum Telekommunikationsgeheimnis usw.
[3] Die Aufzählung ist im Einzelfall anzupassen. So können weitere Unterlagen Weisungscharakter haben oder aufgezählte Typen für einzelne Verantwortliche nicht von Bedeutung sein.

bende Vertraulichkeitsverpflichtung wird durch diese Erklärung nicht berührt.

Die Verpflichtung gilt auch nach Beendigung der Tätigkeit weiter.

Ich bestätige diese Verpflichtung. Ein Exemplar der Verpflichtung habe ich erhalten.

| _____ | _____ | |
|---|---|---|
| Ort, Datum | Unterschrift des Verpflichteten | Unterschrift des Verantwortlichen |