Dossier IV - Verzeichnis von Verarbeitungstätigkeiten

November 2018

Prof. Dr. Anne Riechert

Rechtsgrundlage:

Artikel 30 und Erwägungsgrund 82

Gemäß der Datenschutzgrundverordnung gilt, dass Datenverarbeitungstätigkeiten dokumentiert werden müssen. Dies bedeutet, dass ein Verzeichnis in Schriftform oder in einem elektronischen Format zu führen ist, welches auf Anfrage der Aufsichtsbehörde zur Verfügung gestellt werden muss.

Diese Dokumentationspflichten gelten sowohl für verantwortliche Stellen als auch für Auftragsverarbeiter.

In den folgenden Ausführungen sind nun die rechtlichen Anforderungen eines solches Verzeichnisses dargestellt, die Unternehmen beachten müssen. Im Anschluss (Punkt C.) ist eine Sammlung von weiterführenden Links zu finden, die unter anderem auf Musterverzeichnisse verweist. Dabei sind insbesondere auch die Handreichungen des Bayerischen Landesamts für Datenschutzaufsicht für kleine und mittelständische Unternehmen sowie Vereine berücksichtigt.

A. Was Unternehmen beachten müssen:

- Welche Unternehmen müssen ein Verzeichnis von Verarbeitungstätigkeiten erstellen?

In der Regel müssen alle Unternehmen als Verantwortliche ein Verzeichnis von Verarbeitungstätigkeiten führen.

Artikel 30 Absatz 5 DSGVO beschränkt diese Pflicht zwar unter anderem auf Unternehmen mit einer Größe ab 250 Mitarbeitern. Dies gilt jedoch nicht bei einer regelmäßigen Verarbeitung von Daten. Letzteres kann stets dann in Betracht kommen, wenn beim Verantwortlichen Mitarbeiter beschäftigt sind und deren Daten verarbeitet werden.

- Was muss dokumentiert werden?

Folgende Angaben müssen schriftlich oder in einem elektronischen Format dokumentiert werden:

- Name und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;
- Zwecke der Verarbeitung;
- Beschreibung von Kategorien betroffener Personen und der Kategorien personenbezogener Daten;

- die Kategorien von Empfängern
- Übermittlungen von personenbezogenen Daten an ein Drittland einschließlich de Dokumentierung geeigneter Garantien;
- Löschungsfristen der verschiedenen Datenkategorien
- allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1 Datenschutzgrundverordnung.

- **Welche Vorgaben gibt es seitens der Aufsichtsbehörden?**

Die Datenschutzkonferenz hat Muster für Verarbeitungsverzeichnisse sowohl für verantwortliche Stellen als auch für Auftragsverarbeiter veröffentlicht (https://www.lda.bayern.de/media/dsk_muster_vov_auftragsverarbeiter.pdf - Muster zum Verarbeitungsverzeichnis für Auftragsverarbeiter, Art. 30 Abs. 2 DSGVO sowie https://www.lda.bayern.de/media/dsk_muster_vov_verantwortlicher.pdf - Muster zum Verarbeitungsverzeichnis für verantwortliche Stellen, Art. 30 Abs. 1 DSGVO).

Im Rahmen der Dokumentation muss das verantwortliche Unternehmen berücksichtigen, dass es stets die Rechtmäßigkeit der Verarbeitung nachweisen muss (Artikel 5 Absatz 2 DSGVO). Daher kann es sich darüber hinaus empfehlen, weitere Informationen zu dokumentieren: Diese Dokumentation kann beispielsweise zusätzliche Angaben zur automatisierten Entscheidungsfindung (einschließlich Profiling), zur Rechtsgrundlage oder Angaben im Hinblick auf die berechtigten Interessen der jeweiligen Verarbeitung umfassen (siehe hierzu die Muster der ICO, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation, die etwa den Speicherort der jeweiligen Kategorien von Daten, die Quelle der personenbezogenen Daten oder die Notwendigkeit von Datenschutz-Folgenabschätzungen in das Verzeichnis aufnehmen).

Auch die Beauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen empfiehlt, weitere, dem Verständnis des Verarbeitungsverzeichnisses dienende, Informationen zur Dokumentation datenschutzrelevanter Vorgänge außerhalb des Verarbeitungsverzeichnisses zu erstellen und vorzuhalten. Sie bezieht sich darauf beispielsweise auf ein Sicherheits-und Rechte-und-Rollen-Konzept, ein Wiederanlaufkonzept sowie auf die Dokumentation des Ergebnisses einer gegebenenfalls durchgeführten Datenschutz-Folgenabschätzung. Zur Gewährleistung eines effektiven Datenschutz-Managementsystems und zu Dokumentationszwecken sollte nach Auffassung der Landesdatenschutzbeauftragten zudem in jedem Fall ein schriftliches, internes Verzeichnis von Verarbeitungstätigkeiten erstellt werden, auch wenn dies an sich nicht erforderlich wäre (https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Verfahrensregister/Inhalt/Verarbeitungstaetigkeiten/Verarbeitungstaetigkeiten.html – Stand: August 2018. Achtung - Update: Link ist nicht mehr erreichbar. Die Aufsichtsbehörde stellt nunmehr lediglich die Hinweise der Datenschutzkonferenz zum Abruf bereit: https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Verzeichnis-Verarbeitungstaetigkeiten/Inhalt/Verarbeitungstaetigkeiten/Hinweise-zum-Verzeichnis-von-Verarbeitungstaetigkeiten.pdf. Hierin heißt es: "*Mit der Erstellung des Verzeichnisses der Verarbeitungstätigkeiten sind keinesfalls alle von der DSGVO geforderten Dokumentationspflichten erfüllt. Das Verzeichnis ist nur ein Baustein, um der in Art. 5 Abs. 2 DSGVO normierten Rechenschaftspflicht zu genügen. So müssen bspw. auch das Vorhandensein von Einwilligungen (Art. 7 Abs. 1DS-GVO), die Ordnungsmäßigkeit der gesamten Verarbeitung (Art. 24 Abs. 1DS-GVO) und das Ergebnis von*

Datenschutz-Folgenabschätzungen (Art. 35 Abs. 7 DSGVO) durch entsprechende Dokumentationen nachgewiesen werden. Um Redundanzen zu vermeiden und den Aufwand für die Erstellung und Führung des Verzeichnisses zu reduzieren, können in die einzelnen Beschreibungen Verweise auf bestehende Dokumente aufgenommen werden, insbesondere solche, die im Rahmen des Informationssicherheitsmanagements angelegt wurden, ohne dass diese in das Verzeichnis übernommen werden müssen.“

B. In Kürze

In der Regel müssen alle Unternehmen als Verantwortliche ein Verzeichnis von Verarbeitungstätigkeiten führen. Die Datenschutzkonferenz hat Musterverzeichnisse veröffentlicht ((https://www.lda.bayern.de/media/dsk_muster_vov_auftragsverarbeiter.pdf). Da ein Unternehmen stets die Rechtmäßigkeit der Datenverarbeitung nachweisen können muss (Artikel 5 Absatz 2 DSGVO), kann sich die Erstellung und Vorhaltung zusätzlicher weiterer Dokumentation empfehlen.

Die Artikel-29-Datenschutzgruppe prüft zurzeit außerdem mögliche Ausnahmen für kleine und mittelständische Unternehmen hinsichtlich der Dokumentationspflichten. In diesem Zusammenhang ist darauf hinzuweisen, dass das Bayerische Landesamt für Datenschutzaufsicht bereits Handreichungen veröffentlicht hat, die sich auf kleine Unternehmen fokussieren und entsprechende Musterverzeichnisse für den vereinfachten Regelfall exemplarisch erstellt (https://www.lda.bayern.de/de/kleine-unternehmen.html). Zu beachten sei dabei jedoch, die jeweils fallbezogene Unterscheidung.

C. Weitere Links und Materialien

- **Datenschutzkonferenz:**

  Die Datenschutzkonferenz hat entsprechende Muster für Verarbeitungsverzeichnisse für verantwortliche Stellen sowie Auftragsverarbeiter veröffentlicht. Diese Dokumente sind unter den beiden folgenden Links abrufbar:

  https://www.lda.bayern.de/media/dsk_muster_vov_auftragsverarbeiter.pdf (Muster zum Verarbeitungsverzeichnis für Auftragsverarbeiter, Art. 30 Abs. 2 DSGVO)
  https://www.lda.bayern.de/media/dsk_muster_vov_verantwortlicher.pdf (Muster zum Verarbeitungsverzeichnis für verantwortliche Stellen, Art. 30 Abs. 1 DSGVO)

  Hierzu werden ergänzend entsprechende Ausfüllhinweise zur Verfügung gestellt:

  https://www.lda.bayern.de/media/dsk_hinweise_vov.pdf (Hinweise zum Verzeichnis von Verarbeitungstätigkeiten). Hier sind unter anderem Erläuterungen zum Zweck und zur Form des Verzeichnisses enthalten. Es wird darauf verwiesen, dass die in Artikel 30 DSGVO genannten Ausnahmen nur selten greifen werden. Insbesondere wegen der regelmäßig erfolgenden Lohnabrechnungen werde daher kaum Unternehmen von der Pflicht eines solchen Verzeichnisses generell befreit sein, allenfalls Unternehmen, die diese Tätigkeiten komplett durcheinen Steuerberater erledigen lassen würden sowie eventuell kleinere Vereine. Zudem erfolgt in dem Dokument der Hinweis, dass bei Lohnabrechnungen oder in der Schülerverwaltung mit der Angabe der Konfessionszugehörigkeit zumeist auch gleich besondere Datenkategorien i.S.d. Art. 9 Abs. 1 DS-GVO vorliegen würden.

Darüber hinaus wurde ebenso seitens der Datenschutzkonferenz ein Kurzpapier als Orientierungshilfe veröffentlicht:
https://www.lda.bayern.de/media/dsk_kpnr_1_verzeichnis_verarbeitungstaetigkeiten.pdf

- **GDD (Gesellschaft für Datenschutz und Datensicherheit e.V.)**

Eine Praxishilfe für die Erstellung von Verzeichnissen von Verarbeitungstätigkeiten wurde ebenso von der Gesellschaft für Datenschutz und Datensicherheit e.V. veröffentlicht (Stand: April 2017), https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_5.pdf. Diese enthält einen Überblick darüber, wer zur Erstellung eines Verfahrensverzeichnisses verpflichtet ist und informiert unter anderem dazu wie folgt:

> *"In der Regel müssen alle Verantwortlichen (Unternehmen/Legaleinheiten/Behörden etc.) ein Verzeichnis von Verarbeitungstätigkeiten führen. Gem. Art. 30 Abs. 5 DS-GVO ist diese Pflicht zwar beschränkt auf Unternehmen*
>
> *>mit einer Größe ab 250 Mitarbeitern; oder*
>
> *>mit einem besonderem Risiko bei der Verarbeitung; oder*
>
> *> mit Verarbeitung von sensiblen Daten (Art. 9 und 10 DS-GVO); oder*
>
> *> einer nicht nur gelegentlichen Verarbeitung.*
>
> *Allerdings geht diese Ausnahmeregelung ins Leere. Spätestens bei Zugrundelegung einer regelmäßigen Verarbeitung sind sämtliche Verantwortlichen unabhängig von ihrer Mitarbeiterstärke betroffen."*

Darüber hinaus enthält diese Praxishilfe des GDD ein Musterformular für die Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten.

- **bitkom (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.)**

Ein detailliertes Nachschlagewerk (46 Seiten) wird ebenso von bitkom e.V., Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V., angeboten (Stand 2017):

https://www.bitkom.org/noindex/Publikationen/2018/Leitfaeden/180530-Verzeichnis-von-Verarbeitungstaetigkeiten-nach-Art-30-EU-Datenschutz-Grundverordnung-DS-GVO/180529-LF-Verarbeitungsverzeichnis-online.pdf

In allgemeinen Hinweisen wird etwa erläutert, was unter einer Verarbeitungstätigkeit zu verstehen ist (S. 20), welche Angaben obligatorisch sind oder interne Zusatzangaben im Verarbeitungsverzeichnis darstellen (S. 12 ff.) Auf S. 29 ff. finden sich zudem konkrete Beispiele, etwa zur Verarbeitung von personenbezogenen Daten zum Zwecke von Marketing und Vertrieb. Auf S. 33 ff. ist ein Musterformular eingefügt, welches zusätzlich als Word-Dokument abrufbar ist. Außerdem ist auf S. 35 die Meldung einer Fehlanzeige veröffentlicht, die in dem Falle anwendbar ist, wenn keine personenbezogenen Daten verarbeitet werden. Auf S. 40 ff. sind die entsprechenden Hinweise zu den einzelnen Musterformularen zu finden, auf die innerhalb der jeweiligen Dokumente ebenso verlinkt wird.

- **Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz**

  Unter https://www.datenschutz.rlp.de/de/themenfelder-themen/datenschutz-grundverordnung/verzeichnis-von-verarbeitungstaetigkeiten/stellt der Landesbeauftragte einen Überblick zu den Pflichten bei der Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten bereit. Weiterhin erfolgt in den FAQ unter der Rubrik „Was gilt es beim Verzeichnis von Verarbeitungstätigkeiten zu beachten?“ eine Zusammenfassung der wichtigsten Punkte, https://www.datenschutz.rlp.de/de/themenfelder-themen/datenschutz-grundverordnung/faq/

- **Die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen**

  Die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen stellt unter https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Verfahrensregister/Inhalt/Verarbeitungstaetigkeiten/Verarbeitungstaetigkeiten.html Informationen über die Erstellung eines Verfahrensverzeichnisses zur Verfügung (Stand August 2018 – Link ist nicht mehr abrufbar: Nunmehr erfolgt ausschließlich ein Hinweis auf die Ausführungen der Datenschutzkonferenz: https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Verzeichnis-Verarbeitungstaetigkeiten/Inhalt/Verarbeitungstaetigkeiten/Hinweise-zum-Verzeichnis-von-Verarbeitungstaetigkeiten.pdf). Allgemeine Informationen finden sich unter: https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzbeauftragte/Inhalt/Betriebliche_Datenschutzbeauftragte/Inhalt/Das-neue-Verarbeitungsverzeichnis-nach-Artikel-30-DS-GVO/Das-neue-Verarbeitungsverzeichnis-nach-Artikel-30-DS-GVO.html

- **Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. (gmds)**

  Unter http://ds-gvo.gesundheitsdatenschutz.org/download/verarbeitungstaetigkeitenverzeichnis.pdf sind Hinweise zur Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten veröffentlicht.

- **IHK Saarland**

  https://www.saarland.ihk.de/ihk-saarland/Integrale?SID=CRAWLER&MODULE=Frontend.Media&ACTION=ViewMediaObject&Media.PK=7452&Media.Object.ObjectType=full (Verzeichnis von Verarbeitungstätigkeiten)

Europaweite Links:

- **ICO: Britische Datenschutzbehörde (Information Commissioner's Office)**

  Noch detaillierter als die Musterverzeichnisse der Datenschutzkonferenz sind die (englischsprachigen) Dokumente, die die Datenschutzbeauftragte des Vereinigten Königreichs auf ihrer Webseite veröffentlicht hat. Beide Muster (Verarbeitungsverzeichnis für verantwortliche Stellen sowie für Auftragsverarbeiter) sind unter dem folgenden Link als Excel-Dokument abrufbar:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/

Vorteilhaft ist, dass hier ein Musterbeispiel enthalten ist und innerhalb der entsprechenden Excel-Tabelle detailliert in unterschiedliche Geschäftseinheiten eines Unternehmens unterteilt wird. So findet sich etwa ein Beispiel für die Datenverarbeitung durch die Personalabteilung, welches nicht nur zwischen Daten von Arbeitnehmern und (erfolgreichen/nicht erfolgreichen) Bewerbern unterscheidet, sondern ebenso zwischen unterschiedlichen Kategorien von personenbezogenen Daten und deren Löschungsfristen differenziert (z.B. steuerrechtliche Angaben, Angaben zum Jahresurlaub, Angaben zur Rente, Angaben zur Bankverbindung). Darüber hinaus ist für jede einzelne Kategorie der vorgenannten personenbezogenen Daten die Verarbeitungsgrundlage konkret benannt und entweder unter einen der Verarbeitungstatbestände des Artikel 6 oder Artikel 9 DSGVO eingeordnet, wobei für jede Kategorie außerdem ebenso angegeben wird, ob mit der einzelnen Verarbeitung eine automatisierte Entscheidung verbunden ist und ob eine Datenschutz-Folgenabschätzung durchzuführen ist.

Unternehmen sollten aber berücksichtigen, dass diese Muster der britischen Datenschutzbehörde über die gemäß Artikel 30 Datenschutzgrundverordnung zu dokumentierenden Pflichtangaben hinausgehen (siehe hierzu oben unter dem Punkt "Was Unternehmen bei der Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten beachten müssen"). Dennoch kann sich eine darüber hinausgehende Dokumentation empfehlen, da Unternehmen die Rechtsmäßigkeit der Datenverarbeitung nachweisen müssen (Artikel 5 Absatz 2 DSGVO).

- **Besondere Ausführungen für kleine und mittelständische Unternehmen und Vereine:**

Das Bayerische Landesamt für Datenschutzaufsicht hat Handreichungen veröffentlicht, die sich auf kleine Unternehmen fokussieren und entsprechende Musterverzeichnisse für den vereinfachten Regelfall exemplarisch erstellt. Die Behörde verweist darauf, dass bei dieser Zusammenstellung kein Anspruch auf Vollständigkeit bestehe und daher jeweils die fallbezogene Unterscheidung zu beachten sei:

https://www.lda.bayern.de/de/kleine-unternehmen.html

Im Einzelnen:

Für Vereine:

https://www.lda.bayern.de/media/muster_1_verein.pdf (Anforderungen)

https://www.lda.bayern.de/media/muster_1_verein_verzeichnis.pdf (Musterverzeichnis für Verarbeitungstätigkeiten)

Für Handwerksbetriebe:

https://www.lda.bayern.de/media/muster_3_handwerksbetrieb.pdf (Anforderungen)

https://www.lda.bayern.de/media/muster_3_handwerksbetrieb_verzeichnis.pdf (Musterverzeichnis für Verarbeitungstätigkeiten)

Im Hinblick auf Handwerksbetriebe werden die Informationen des Bayerischen Landesamts für Datenschutzaufsicht durch den Zentralverband des Deutschen Handwerks (ZDH) ergänzt, der die entsprechenden Dokumentationspflichten näher erläutert, abrufbar unter: https://www.zdh.de/fileadmin/user_upload/themen/Recht/Datenschutz/Handwerksbetriebe/ZDH_Praxis_Datenschutz_Dokumentationspflich_Handwerksbetriebe.pdf), und unter den nachfolgenden Links Musterverzeichnisse für Verarbeitungstätigkeiten für Handwerksbetriebe zur Verfügung stellt:
https://www.zdh.de/fileadmin/user_upload/themen/Recht/Datenschutz/Handwerksbetriebe/Anlage_1_Muster_Verarbeitsungsverzeichnis_Handwerksbetriebe.docx (Musterverzeichnis für Verarbeitungstätigkeiten)
https://www.zdh.de/fileadmin/user_upload/themen/Recht/Datenschutz/Handwerksbetriebe/Anlage_2_Beispiel_Verarbeitsungsverzeichnis_Handwerksbetriebe.docx (Beispiel Musterverzeichnis für Verarbeitungstätigkeiten)
https://www.zdh.de/fileadmin/user_upload/themen/Recht/Datenschutz/Handwerksbetriebe/Anlage_3_Liste_technischer_organisatorischer_Massnahmen.docx (Technische und organisatorische Maßnahmen)
Mehr Informationen und Unterlagen zur Datenschutzgrundverordnung finden Handwerksbetriebe unter https://www.zdh.de/fachbereiche/organisation-und-recht/datenschutz/datenschutz-fuer-handwerksbetriebe/

Für Kfz-Werkstätten:

https://www.lda.bayern.de/media/muster_2_kfz-werkstatt.pdf (Anforderungen)

https://www.lda.bayern.de/media/muster_2_kfz-werkstatt_verzeichnis.pdf (Musterverzeichnis für Verarbeitungstätigkeiten)

Für Steuerberater:

https://www.lda.bayern.de/media/muster_4_steuerberater.pdf (Anforderungen)

Für Arztpraxen:

https://www.lda.bayern.de/media/muster_5_arztpraxis.pdf (Anforderungen)

https://www.lda.bayern.de/media/muster_5_arztpraxis_verzeichnis.pdf (Musterverzeichnis für Verarbeitungstätigkeiten)

Für WEG-Verwaltungen:

https://www.lda.bayern.de/media/muster_6_weg-verwaltung.pdf (Anforderungen)

https://www.lda.bayern.de/media/muster_6_weg-verwaltung_verzeichnis.pdf (Musterverzeichnis für Verarbeitungstätigkeiten)

Für Produktionsbetriebe:

https://www.lda.bayern.de/media/muster_7_produktionsbetrieb.pdf (Anforderungen)

Für Genossenschaftsbanken:

https://www.lda.bayern.de/media/muster_8_genossenschaftsbank.pdf (Anforderungen)

Für Online-Shops:

https://www.lda.bayern.de/media/muster_9_online-shop.pdf (Anforderungen)

https://www.lda.bayern.de/media/muster_9_online-shop_verzeichnis.pdf (Musterverzeichnis für Verarbeitungstätigkeiten)

Für Bäckereien:

https://www.lda.bayern.de/media/muster_10_baeckerei.pdf (Anforderungen)

Für Beherbungsbetriebe:

https://www.lda.bayern.de/media/muster_11_beherbergungsbetrieb.pdf (Anforderungen)

https://www.lda.bayern.de/media/muster_11_beherbergungsbetrieb_verzeichnis.pdf (Musterverzeichnis für Verarbeitungstätigkeiten)

Für Einzelhändler:

https://www.lda.bayern.de/media/muster_12_einzelhaendler.pdf (Anforderungen)

https://www.lda.bayern.de/media/muster_12_einzelhaendler_verzeichnis.pdf (Musterverzeichnis für Verarbeitungstätigkeiten)