AdOrga Solutions

# Beschäftigtendatenschutz

## Background-Check und Datenscreening von Bewerbern und Beschäftigten

Autorin:
Regina Mühlich

Stand:
April 2023

# Inhaltsverzeichnis

**1 Einleitung ... 2**
1.1 Grundsätze ... 2
1.2 Beschäftigte ... 2
**2 Background-Checks ... 3**
2.1 Überblick ... 3
2.2 Grundsatz der Direkterhebung und Erforderlichkeit ... 3
2.3 Judikatur ... 4
2.4 Fazit ... 4
**3 Terrorlistenscreening ... 4**
3.1 Überblick ... 4
3.2 Datenabgleich ... 5
3.3 Verhältnismäßigkeit ... 5
3.4 Judikatur ... 6
3.5 Fazit ... 6
**4 Handlungsempfehlungen ... 6**
**5 Weiterführende Links ... 7**
**6 Autorin ... 8**

* Hinweis: Der Übersichtlichkeit wegen wurden nur männliche Formen verwendet.



Wir möchten darauf hinweisen, dass die Nutzung der Informationen dieses Dokumentes, auch auszugsweise, oder die Weitergabe an Dritte die Zustimmung der Autoren bedarf.

# 1 Einleitung

## 1.1 Grundsätze

Die Datenschutz-Grundverordnung (DSGVO) enthält eine Öffnungsklausel für eine eigenständige nationale Regelung zum Schutz personenbezogener Daten im Beschäftigungsverhältnis. Der deutsche Gesetzgeber hat von dieser Öffnungsklausel Gebrauch gemacht: § 26 Bundesdatenschutzgesetz (BDSG). Diese Regelung ist nahezu identisch mit § 32 BDSG a.F. Seit Jahren wird in Deutschland über ein Gesetz für den Beschäftigtendatenschutz diskutiert.[1]

## 1.2 Beschäftigte

Beschäftigte sind nicht nur Arbeitnehmer, sondern auch zur Berufsbildung Beschäftigte, Werkstudenten, Leiharbeitnehmer sowie Personen, die wegen ihrer wirtschaftlichen Unselbstständigkeit als arbeitnehmerähnliche Personen anzusehen sind.

§ 26 Abs. 8 BDSG definiert:

(8) *Beschäftigte im Sinne dieses Gesetzes sind:*

1. *Arbeitnehmerinnen und Arbeitnehmer, einschließlich der Leiharbeitnehmerinnen und Leiharbeitnehmer im Verhältnis zum Entleiher,*
2. *zu ihrer Berufsbildung Beschäftigte,*
3. *Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitandinnen und Rehabilitanden),*
4. *in anerkannten Werkstätten für behinderte Menschen Beschäftigte,*
5. *Freiwillige, die einen Dienst nach dem Jugendfreiwilligen-dienstegesetz oder dem Bundesfreiwilligendienstgesetz leisten,*
6. *Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,*
7. *Beamtinnen und Beamte des Bundes, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende.*

Im Sinne des Datenschutzrechts gelten Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist, ebenfalls als Beschäftigte.

[1] Brauchen wir ein Gesetz zum Beschäftigtendatenschutz https://www.bund-verlag.de/aktuelles~Brauchen-wir-ein-Gesetz-zum-Beschaeftigtendatenschutz-~.html (zuletzt aufgerufen am 11.04.2023)



Wir möchten darauf hinweisen, dass die Nutzung der Informationen dieses Dokumentes, auch auszugsweise, oder die Weitergabe an Dritte die Zustimmung der Autoren bedarf.

Der Begriff „Beschäftigte“ ist im Datenschutzrecht weitgefasst: Bewerber, Leiharbeiter, Werkstudenten, etc. zählen dazu wie auch ausgeschiedene Mitarbeiter.

# 2 Background-Checks

## 2.1 Überblick

Die **Suche nach Informationen** über Bewerberinnen und Bewerber im Internet ist für Personalabteilungen und Personalverantwortliche keine Seltenheit. In sozialen Netzwerken wie Twitter, Xing und LinkedIn oder in Internet-Suchmaschinen lassen sich vielfältige Informationen über Bewerber finden. Die dabei gesammelten Daten können sowohl einen privaten als auch einen beruflichen Hintergrund haben. Zudem können die Daten vom Bewerber selbst und/oder von Dritten auf der Plattform oder im Internet veröffentlicht worden sein. Dabei sind nicht alle Veröffentlichungen, d.h. Daten, die der Bewerber seiner Privatsphäre zuordnet, zur Kenntnisnahme durch potenzielle Arbeitgeber bestimmt.

Letztendlich kann der (zukünftige) Arbeitgeber durch eine Internetrecherche ein umfassendes Persönlichkeitsprofil des (zukünftigen) Beschäftigten erstellen. Neben Ausbildung und Berufsweg lassen sich auch private Neigungen oder Vorlieben des Bewerbers recherchieren.

Der Arbeitgeber kann durch den „Internet-Background-Check“ auch negative Informationen generieren. Für den Bewerber kann dies ebenfalls nachteilig sein und zur Ablehnung seiner Bewerbung führen. In vielen Fällen wird der Bewerber gar nicht erst zu einem Vorstellungsgespräch eingeladen, so dass er die tatsächlichen Ablehnungsgründe nicht kennt.

Schon aus diesem Grund ist eine Internetrecherche über den Bewerber nur unter bestimmten Voraussetzungen zulässig.

## 2.2 Grundsatz der Direkterhebung und Erforderlichkeit

Im Bewerberauswahlverfahren gilt grundsätzlich der **Grundsatz der Direkterhebung**. Eine Zuverlässigkeitsüberprüfung greift stark in das Persönlichkeitsrecht des Betroffenen ein. Schon aus Gründen der Verhältnismäßigkeit dürfen Background Checks nur unter strengen Zulässigkeitsvoraussetzungen durchgeführt werden. Die Informationen müssen daher grundsätzlich direkt beim Bewerber eingeholt werden. Dies setzt entweder die aktive Mitwirkung des Bewerbers oder zumindest seine Kenntnis vor der Datenerhebung voraus.

Background-Checks dürfen nur unter strengen Voraussetzungen durchgeführt werden. Im Rahmen des Bewerberverfahrens sind zwei Ausnahmetatbestände denkbar, in denen die Datenerhebung ohne Kenntnis des Bewerbers zulässig ist und wenn dies für die



Wir möchten darauf hinweisen, dass die Nutzung der Informationen dieses Dokumentes, auch auszugsweise, oder die Weitergabe an Dritte die Zustimmung der Autoren bedarf.

Entscheidung über die Begründung eines Beschäftigungsverhältnisses erforderlich ist (§ 26 Abs. 1 S. 1 BDSG).

Die Erforderlichkeit ist im **konkreten Einzelfall**, d.h. für jede einzelne Bewerbung, zu prüfen. Nur bei Vorliegen besonderer Umstände kann der Arbeitgeber daher einen Background-Check rechtfertigen. Vom Grundsatz der Direktanfrage kann auch abgewichen werden, wenn eine gesetzliche Regelung besteht. Nur wenn der Arbeitgeber auf einen Ausnahmetatbestand zurückgreifen kann, lässt sich eine Internetrecherche über den Bewerber datenschutzrechtlich legitimieren.

Der Verantwortliche (hier: Arbeitgeber) hat auch beim Bewerberauswahlverfahren seinen Informationspflichten nachzukommen (Art. 13 Abs. 1, 2 DS-GVO).
Bei Dritterhebungen entstehen ebenfalls Informationspflichten; dies vor allem auch im Hinblick der Zweckänderung bei Internetrecherche (Art. 14 Abs. 4 DS-GVO).

### 2.3 Judikatur

LAG Baden-Württemberg, Urt. v. 21.02.2019 – 3 Sa 65/17 – Background-Check auch auf Social-Media bei Verdachtsmomenten

*Macht der Bewerber unrichtige Angaben über seine Qualifikationen, kann der Arbeitgeber den Arbeitsvertrag anfechten, nachdem er sich im Internet weitere Informationen über ihn eingeholt hatte. Der Abgleich der Bewerberdaten mit Angaben in privaten sozialen Netzwerken (wie z.B. Facebook) war hier ausnahmsweise zulässig.*

### 2.4 Fazit

Die Datenerhebung darf regelmäßig nicht hinter dem Rücken des Bewerbers erfolgen. Es gilt grundsätzlich der Grundsatz der Direkterhebung und der der Transparenz – der Bewerber muss vor Verarbeitung und Übermittlung seiner Daten wissen, zu welchen Zwecken diese verwendet werden (Informationspflichten Artt. 12 ff. DS-GVO).

## 3 Terrorlistenscreening

### 3.1 Überblick

Der **Kampf gegen den internationalen Terrorismus** gewinnt immer mehr an Bedeutung. Die EU hat zwei Verordnungen erlassen, die darauf abzielen, Geschäftskontakte mit terrorverdächtigen Personen und Organisationen umfassend zu unterbinden. Die beiden EU-Anti-Terrorismus-Verordnungen (2580/2001/EG und 881/2002/EG) enthalten Sanktionslisten, in denen alle terroristischen Organisationen und Personen aufgeführt sind.[2]

[2] https://www.eeas.europa.eu/eeas/european-union-sanctions_en (zuletzt aufgerufen am 18.04.2023)



Wir möchten darauf hinweisen, dass die Nutzung der Informationen dieses Dokumentes, auch auszugsweise, oder die Weitergabe an Dritte die Zustimmung der Autoren bedarf.

Die EU-Anti-Terrorismusverordnungen verbieten die Bereitstellung von Geldern an Unternehmen, Organisationen und Personen, die auf den Terrorlisten aufgeführt sind. Diese sogenannten Bereitstellungsverbote wirken sich unmittelbar auf Arbeitsverhältnisse aus. Ein Unternehmen darf einem Mitarbeiter, der auf einer Terrorliste aufgeführt ist, kein Arbeitsentgelt zahlen. Dies bedeutet in der Konsequenz, dass ein Arbeitgeber einem Bewerber auch keine Reisekosten oder sonstige Auslagen erstatten darf.

Einer gelisteten Person dürfen weder direkt noch indirekt Gelder oder wirtschaftliche Ressourcen zur Verfügung gestellt werden.

**Arbeitgeber sind daher verpflichtet, zu überprüfen**, ob Mitarbeiter und Bewerber auf den EU-Terrorlisten stehen. Diese Überprüfungen sind jedoch aus datenschutzrechtlicher Sicht nicht unproblematisch.

### 3.2 Datenabgleich

Der Datenabgleich kann grundsätzlich rechtmäßig durchgeführt werden. Die Einhaltung des Bereitstellungsverbots könnte ansonsten ohne ein Datenscreening durch die Unternehmen nicht gewährleistet werden, was wiederum eine Ordnungswidrigkeit darstellt und Sanktionen für das Unternehmen, den Arbeitgeber, nach sich ziehen würden.

Der Datenabgleich ist nicht auf konkrete Verdachtsfälle beschränkt, da der Arbeitgeber erst durch den Abgleich erfährt, ob sich unter den Bewerbern und/oder Beschäftigten ein Terrorverdächtiger befindet. Es wäre daher geradezu kontraproduktiv, wenn der Abgleich unter dem Gesichtspunkt des Datenschutzes unzulässig wäre.

Ein Datenabgleich mit den Terrorlisten der USA wird hingegen nicht zulässig sein. Insbesondere können sich Terrorverdächtige nicht mit Rechtsmitteln gegen eine unberechtigte Nennung auf einer US-Terrorliste wehren. Bei einer unberechtigten Nennung auf einer EU-Terrorliste steht dem Betroffenen der Weg zum EuGH offen, um eine Streichung von der Sanktionsliste zu erreichen. Ein vergleichbares rechtsstaatliches Verfahren ermöglichen die USA bei ihren Terrorlisten nicht. Zudem ist bei den US-Terrorlisten - im Gegensatz zu den EU-Terrorlisten - nicht klar, aus welchen Quellen sich die Inhalte der Listen zusammensetzen.[3]

### 3.3 Verhältnismäßigkeit

Der Grundsatz der Verhältnismäßigkeit ist auch beim Datenabgleich mit den Terrorlisten in vollem Umfang zu beachten und einzuhalten. Die in der DS-GVO und im BDSG beschriebenen Zulässigkeitskriterien werden bei der Durchführung des Terrorlistenscreenings nicht eingeschränkt. Dies bedeutet, dass in der Regel nicht alle in der Terrorliste enthaltenen Daten mit den Bewerber- und Beschäftigtendaten abgeglichen

[3] Vgl. Byers, P. (2022), Mitarbeiterkontrollen, Rn. 315, Verlag C.H. Beck oHG München.



Wir möchten darauf hinweisen, dass die Nutzung der Informationen dieses Dokumentes, auch auszugsweise, oder die Weitergabe an Dritte die Zustimmung der Autoren bedarf.

werden dürfen. Zur Identifizierung der in der Terrorliste aufgeführten Person wird in der Regel bereits eine Auswertung des Vor- und Nachnamens möglich und ausreichend sein. Erst wenn sich aus dem ersten Datenabgleich ein konkreter Tatverdacht ergibt, ist die Auswertung weiterer personenbezogener Daten wie z.B. Staatsangehörigkeit, Geburtsdatum, Personalausweisnummer verhältnismäßig und datenschutzrechtlich zulässig. Ohne Vorliegen eines konkreten Tatverdachts ist ein weiterer Datenabgleich rechtswidrig. Der Umfang der Datenauswertung bei einem Terrorlistenscreening ist daher unbedingt zu begrenzen.

### 3.4 Judikatur

Bundesfinanzhof, Urt. v. 19.06.2012 – VII R 43/11

*Die Rechtsgrundlage findet sich in § 26 Abs. 1 S. 1 BDSG: Der Abgleich der personenbezogenen Daten der Bediensteten mit dem Namen in den Listen für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder für dessen Begründung, Durchführung oder Beendigung erforderlich, da Unternehmen gemäß § 34 Abs. 4 des Außenwirtschaftsgesetzes (AWG) unter Strafandrohung keine Bediensteten beschäftigen dürfen, die in den Listen aufgeführt sind.*

### 3.5 Fazit

Für die Beurteilung der Verhältnismäßigkeit des Datenabgleichs ist daher die Häufigkeit des Screenings ein wichtiges Kriterium. Es setzt sich die Auffassung durch, dass ein jährlicher Abgleich der Mitarbeiterdaten mit den EU-Terrorlisten in der Regel ausreichend und damit verhältnismäßig ist (vgl. Dienstvorschrift des Bundesministeriums „Zugelassener Wirtschaftsbeteiligter - AEO“[4]). Danach ist es für die Zuerkennung des AEO-Status ausreichend, wenn die Sicherheitsüberprüfung einmal jährlich durchgeführt wird. Dieser Grundsatz ist auf das Terrorlistenscreening im Beschäftigungsverhältnis übertragbar. Ein ständiger und dauerhafter Datenabgleich greift regelmäßig unverhältnismäßig in die Persönlichkeitssphäre des Arbeitnehmers ein.[5]

## 4 Handlungsempfehlungen

- Die Zulässigkeit eines Background-Checks ist im Einzelfall zu prüfen.
- Die Erforderlichkeit und Verhältnismäßigkeit eines Datenabgleichs beim Screening, ist regelmäßig zu überprüfen.

[4] https://www.zoll.de/DE/Fachthemen/Zoelle/Zugelassener-Wirtschaftsbeteiligter-AEO/zugelassener-wirtschaftsbeteiligter-aeo_node.html (zuletzt aufgerufen am 06.02.2023)

[5] Vgl. Byers, P. (2022), Mitarbeiterkontrollen, Rn. 319, Verlag C.H. Beck oHG München.



Wir möchten darauf hinweisen, dass die Nutzung der Informationen dieses Dokumentes, auch auszugsweise, oder die Weitergabe an Dritte die Zustimmung der Autoren bedarf.

- Eine Datenschutz-Folgenabschätzung ist aufgrund des starken Eingriffs in die Privatsphäre der betroffenen Personen, sowohl für Background-Checks als auch für das Terrorlistenscreening dringend anzuraten (Art. 35 DS-GVO).
- Die Prozesse sind im Verzeichnis der Verarbeitungstätigen zu dokumentieren und regelmäßig zu überprüfen.
- Die Mitarbeiter der Personalabteilung sowie die Führungskräfte, die an der Bewerberauswahl beteiligt sind, sind regelmäßig für Background-Checks und Internetrecherche zu sensibilisieren.
- Die Mitarbeiter der Personalabteilung sind regelmäßig in der Durchführung des Screenings zu schulen.
- Der betriebliche Datenschutzbeauftragte ist bei Änderungen und für Bewertungen früh- und rechtzeitig einzubinden.

## 5 Weiterführende Links

- European Union Sanctions
  https://www.eeas.europa.eu/eeas/european-union-sanctions_en
  (zuletzt aufgerufen am 11.04.2023).
- Zugelassener Wirtschaftsbeteiligter (AEO)
  https://www.zoll.de/DE/Fachthemen/Zoelle/Zugelassener-Wirtschaftsbeteiligter-AEO/zugelassener-wirtschaftsbeteiligter-aeo_node.html
  (zuletzt aufgerufen am 11.04.2023).

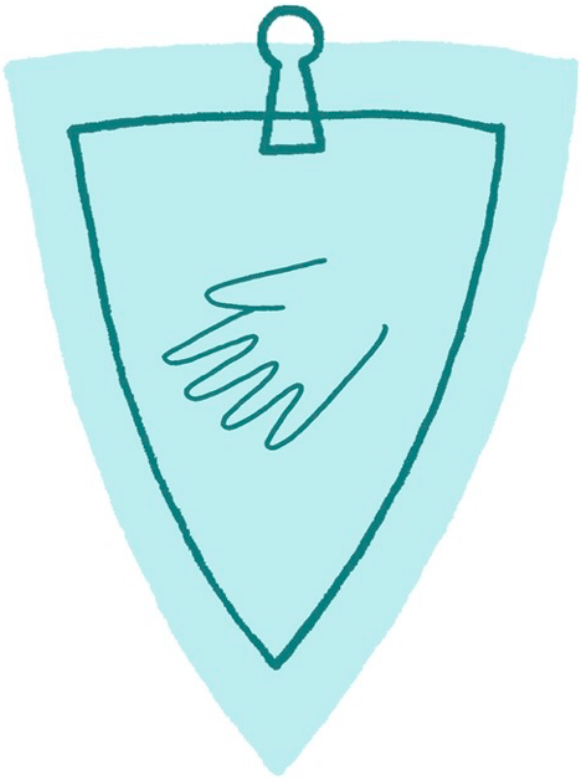
Hinweise: https://www.firesafecouncil.org/employers-in-the-european-union-may-conduct-background-checks-but-must-comply-with-local-law/



Wir möchten darauf hinweisen, dass die Nutzung der Informationen dieses Dokumentes, auch auszugsweise, oder die Weitergabe an Dritte die Zustimmung der Autoren bedarf.

# 6 Autorin

**Regina Mühlich** ist Wirtschaftsjuristin und Geschäftsführerin der AdOrga Solutions GmbH und seit über 20 Jahren im Datenschutz tätig. Sie ist zert. Datenschutzbeauftragte, CIPM (IAPP), anerkannte und geprüfte Sachverständige für Systeme und Anwendungen der Informationsverarbeitung im kaufmännisch-administrativen Bereichen (IT) und für Datenschutz, Informationssicherheitsbeauftragte (TÜV), IT Security Fundamentals in ISO 27001, Penetration Testing & Forensic Investigation (ICO Certificate, ID 003E1KQR), Scrum Master (PMI), zert. Compliance Officer sowie Auditorin für Datenschutz. Als externe Datenschutzbeauftragte und Compliance Officer berät und unterstützt sie mit ihrem Team nationale und internationale Unternehmen aus unterschiedlichsten Branchen. Sie ist Advisory Board Member of health-h sowie Vorständin des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e. V.



(Bildquelle: © AdOrga Solutions GmbH)

© Copyright 2023 Regina Mühlich I AdOrga Solutions GmbH I E-Mail: consulting@adogasolutions.de

Dieses Dokument ist urheberrechtlich geschütztes Eigentum. Jede Verwertung, auch auszugsweise, außerhalb der engen Grenzen des Urhebergesetzes ist ohne schriftliche Zustimmung der Autorin unzulässig und strafbar.

Dies gilt insbesondere für die Vervielfältigung, Verarbeitung und Verwendung für Vorträge.

Dieses Dokument ist auf dem Stand des ersten Tages der Veröffentlichung und kann von der Autorin jederzeit geändert werden. Die Informationen in diesem Dokument sind ohne jegliche Garantie, ausdrücklich oder implizit, einschließlich ohne Gewährleistung der Eignung für einen bestimmten Zweck.



Wir möchten darauf hinweisen, dass die Nutzung der Informationen dieses Dokumentes, auch auszugsweise, oder die Weitergabe an Dritte die Zustimmung der Autoren bedarf.