

# Das Verzeichnis der Bearbeitungstätigkeiten gemäss Artikel 12 nDSG

Handreichung

Stand: 22.06.2023

## *Wichtige Informationen zu diesem Dokument*

Bitte beachten Sie, dass es sich bei dem hier dargestellten Inhalt um grundlegende Informationen handelt, die an den jeweiligen Einzelfall individuell anzupassen sind. Die DATA Security AG ist um Richtigkeit und Aktualität der in diesem Dokument bereitgestellten Informationen bemüht. Wir können jedoch keine Haftung dafür übernehmen, dass der Inhalt für den jeweils individuellen Sachverhalt uneingeschränkt verwendbar, fehlerfrei und aktuell ist. Die unkritische Übernahme der Inhalte erfolgt auf eigenes Risiko und ersetzt keineswegs die ggf. notwendige individuelle rechtliche Beratung im konkreten Fall. Wir weisen darauf hin, dass dieses von der DATA Security AG bereitgestellte Dokument keinerlei Rechtsberatung darstellt und dazu auch nicht intendiert ist.

## Kommentar:

Der Begriff «Bearbeitung» wird in **Artikel 5 Buchstabe d nDSG (Begriffe)** präzisiert und bezeichnet «Bearbeiten» als jeden Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten verstanden.

Diese umfassende Definition stellt ein Unternehmen vor grosse Herausforderungen, denn dort werden überall und ständig Personendaten bearbeitet.

Die Datenbearbeitungsvorgänge innerhalb eines Unternehmens werden über das Bearbeitungsverzeichnis abgebildet; es dient quasi als «Cockpit» der «Bearbeitungstätigkeiten» eines Unternehmens und soll eine Übersicht der Bearbeitungsvorgänge verschaffen, denn das Unternehmen muss sich darüber bewusst sein, welche Daten, von welcher Abteilung, von welchen Personen und zu welchem Zweck (gespeichert und) bearbeitet werden.

Das Bearbeitungsverzeichnis dient demnach als Nachweis, dass sämtliche Bearbeitungsvorgänge nachvollzogen und belegt werden können, und dass die datenschutzrechtlichen Vorgaben entsprechend und vollständig erfüllt sind. Nicht zuletzt ist damit für das Unternehmen Transparenz und rechtliche Absicherung gewährleistet.

## Verpflichtung

Gemäss **Artikel 12 nDSG (Verzeichnis der Bearbeitungstätigkeiten)** haben sowohl Verantwortliche als auch Auftragsbearbeiter je ein Verzeichnis ihrer Bearbeitungstätigkeiten zu führen.

Das Bearbeitungsverzeichnis ist jedoch nicht immer Pflicht.

Eine Ausnahme ist im nDSG dann für Unternehmen vorgesehen, wenn sie weniger als 250 Angestellte beschäftigen und deren Datenbearbeitung ein «geringes» Risiko für Verletzungen der Persönlichkeit der betroffenen Personen bedeutet.

Sicherlich kann man aber in diesem Kontext **nicht** von einem von einem «geringen» Risiko ausgehen, wenn das Unternehmen Folgendes durchführt:

- Besonders schützenswerte Personendaten, beispielsweise Gesundheitsdaten – [siehe **Artikel 5 Buchstabe c nDSG (Begriffe)**] – werden in grossem Umfang bearbeitet.
- (Und/oder) es findet ein Profiling mit hohem Risiko statt.

## Aufbau

Zweck des Bearbeitungsverzeichnisses ist die Schaffung einer Übersicht über sämtlicher Bearbeitungstätigkeiten. Im nDSG werden hierzu folgende Mindestinhalte vorgegeben:

- Die Identität des Verantwortlichen.
- Bearbeitungszwecke(e).
- Beschreibung der Kategorien betroffener Personen sowie der Kategorien bearbeiteter Personendaten.
- Kategorien der Empfänger der Personendaten.
- Wenn möglich, die Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer.
- Wenn möglich, eine allgemeine Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit – hier wird Bezug auf die sogenannten erforderlichen «technischen und organisatorischen Massnahmen» (TOM) zum Datenschutz genommen. [Siehe Artikel 3 nDSV (Technische und organisatorische Massnahmen)]

- Wenn die Personendaten ins Ausland bekanntgegeben werden, müssen der (jeweilige) Staat bzw. das jeweilige internationale Organ namentlich aufgeführt sowie bestimmte Garantien für die Sicherheit der Personendaten in diesem Zusammenhang angegeben werden.

## Form

Weder im nDSG noch in der nDSV (neue Datenschutz-Verordnung) werden Vorgaben zur Form des Bearbeitungsverzeichnisses gemacht. Typisch ist ein elektronisches Format, beispielsweise als Excel-Tabelle oder Word-Dokument.

## Einsicht in das Bearbeitungsverzeichnis

Beim Bearbeitungsverzeichnis handelt es sich um ein rein internes Dokument.

Jedoch kann der EDÖB im Rahmen einer Untersuchung die Bearbeitungsvorgänge anhand des Verzeichnisses kontrollieren. Hierzu sollte das Bearbeitungsverzeichnis der Aufsichtsbehörde einen kurzen Überblick über sämtliche Bearbeitungstätigkeiten im Unternehmen liefern können und dient dem EDÖB zum Nachweis, dass die datenschutzrechtlichen Vorschriften eingehalten wurden.

# Relevante Gesetzestexte

Quelle 1: [EDÖB nDSG online \(abgerufen im Juni 2023\)](#)

Quelle 2: [EDÖB nDSV online \(abgerufen im Juni 2023\)](#)

## Art. 5 Begriffe nDSG

In diesem Gesetz bedeuten:

- a. **Personendaten:** alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen;
- b. **betroffene Person:** natürliche Person, über die Personendaten bearbeitet werden;
- c. **besonders schützenswerte Personendaten:**
  - 1. Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten,
  - 2. Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie,
  - 3. genetische Daten,
  - 4. biometrische Daten, die eine natürliche Person eindeutig identifizieren,
  - 5. Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen,
  - 6. Daten über Massnahmen der sozialen Hilfe;
- d. **Bearbeiten:** jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten;
- e. **Bekanntgeben:** das Übermitteln oder Zugänglichmachen von Personendaten;
- f. **Profiling:** jede Art der automatisierten Bearbeitung von Personendaten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;
- g. **Profiling mit hohem Risiko:** Profiling, das ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringt, indem es zu einer Verknüpfung von Daten führt, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt;
- h. **Verletzung der Datensicherheit:** eine Verletzung der Sicherheit, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden;
- i. **Bundesorgan:** Behörde oder Dienststelle des Bundes oder Person, die mit öffentlichen Aufgaben des Bundes betraut ist;
- j. **Verantwortlicher:** private Person oder Bundesorgan, die oder das allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung entscheidet;
- k. **Auftragsbearbeiter:** private Person oder Bundesorgan, die oder das im Auftrag des Verantwortlichen Personendaten bearbeitet.

## Art. 12 Verzeichnis der Bearbeitungstätigkeiten nDSG

1 Die Verantwortlichen und Auftragsbearbeiter führen je ein Verzeichnis ihrer Bearbeitungstätigkeiten.

2 Das Verzeichnis des Verantwortlichen enthält mindestens:

- a. die Identität des Verantwortlichen;
- b. den Bearbeitungszweck;
- c. eine Beschreibung der Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten;
- d. die Kategorien der Empfängerinnen und Empfänger;
- e. wenn möglich die Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer;
- f. wenn möglich eine allgemeine Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit nach Artikel 8;
- g. falls die Daten ins Ausland bekanntgegeben werden, die Angabe des Staates sowie die Garantien nach Artikel 16 Absatz 2.

3 Das Verzeichnis des Auftragsbearbeiters enthält Angaben zur Identität des Auftragsbearbeiters und des Verantwortlichen, zu den Kategorien von Bearbeitungen, die im Auftrag des Verantwortlichen durchgeführt werden, sowie die Angaben nach Absatz 2 Buchstaben f und g.

4 Die Bundesorgane melden ihre Verzeichnisse dem EDÖB.

5 Der Bundesrat sieht Ausnahmen für Unternehmen vor, die weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen und deren Datenbearbeitung ein geringes Risiko von Verletzungen der Persönlichkeit der betroffenen Personen mit sich bringt.

## Art. 3 Technische und organisatorische Massnahmen nDSV

1 Um die Vertraulichkeit zu gewährleisten, müssen der Verantwortliche und der Auftragsbearbeiter geeignete Massnahmen treffen, damit:

- a. berechnete Personen nur auf diejenigen Personendaten Zugriff haben, die sie zur Erfüllung ihrer Aufgaben benötigen (Zugriffskontrolle);
- b. nur berechnete Personen Zugang zu den Räumlichkeiten und Anlagen haben, in denen Personendaten bearbeitet werden (Zugangskontrolle);
- c. unbefugte Personen automatisierte Datenbearbeitungssysteme nicht mittels Einrichtungen zur Datenübertragung benutzen können (Benutzerkontrolle).

2 Um die Verfügbarkeit und Integrität zu gewährleisten, müssen der Verantwortliche und der Auftragsbearbeiter geeignete Massnahmen treffen, damit:

- a. unbefugte Personen Datenträger nicht lesen, kopieren, verändern, verschieben, löschen oder vernichten können (Datenträgerkontrolle);
- b. unbefugte Personen Personendaten im Speicher nicht speichern, lesen, ändern, löschen oder vernichten können (Speicherkontrolle);
- c. unbefugte Personen bei der Bekanntgabe von Personendaten oder beim Transport von Datenträgern Personendaten nicht lesen, kopieren, verändern, löschen oder vernichten können (Transportkontrolle);
- d. die Verfügbarkeit der Personendaten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können (Wiederherstellung);
- e. alle Funktionen des automatisierten Datenbearbeitungssystems zur Verfügung stehen (Verfügbarkeit), Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte Personendaten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität);

- f. Betriebssysteme und Anwendungssoftware stets auf dem neusten Sicherheitsstand gehalten und bekannte kritische Lücken geschlossen werden (Systemsicherheit).

3 Um die Nachvollziehbarkeit zu gewährleisten, müssen der Verantwortliche und der Auftragsbearbeiter geeignete Massnahmen treffen, damit:

- a. überprüft werden kann, welche Personendaten zu welcher Zeit und von welcher Person im automatisierten Datenbearbeitungssystem eingegeben oder verändert werden (Eingabekontrolle);
- b. überprüft werden kann, wem Personendaten mit Hilfe von Einrichtungen zur Datenübertragung bekanntgegeben werden (Bekanntgabekontrolle);
- c. Verletzungen der Datensicherheit rasch erkannt (Erkennung) und Massnahmen zur Minderung oder Beseitigung der Folgen ergriffen werden können (Beseitigung).