## Inventar – Überblick der Datenbearbeitungen

**Formular B.1**

Unternehmenseinheit: _____ Ausgefüllt von: _____ Stand vom: _____

**Arbeitsanweisung:**

- Auf diesem Formular wird **jede Datenbearbeitung** (→ Glossar) im Unternehmen einzeln mit einer Kurzbezeichnung (z.B. Personaladministration, Lagerbewirtschaftung, Unternehmenswebsite, Online-Shop, CRM, Whistleblowing-Datenbank, Vertragsmanagement) oder dem intern verwendeten Namen oder Akronym aufgeführt. Es existiert noch keine offizielle Liste der typischen Datenbearbeitungen von Unternehmen, allerdings kann hier das Beispiel ganz am Ende dieses Formular sowie die Liste der **Standardanwendungen** unter dem bisherigen österreichischen Datenschutzrecht ~~Hinweise liefern~~ (siehe beispielsweise hier~~).~~) Hinweise liefern.

- Jede Datenbearbeitung erhält eine **eineindeutige Nummer** zugewiesen (die "DB-Nr."). Wie diese Nummer aufgebaut ist und wie sie vergeben wird, spielt keine Rolle. Sie wird jedoch benutzt, um die betreffende Datenbearbeitung auf den anderen Formularen zu identifizieren.

- Die **Reihenfolge** der Datenbearbeitungen spielt auch keine Rolle. Dieser Überblick kann auch in einer **separaten Datei** verwaltet werden. Aufzuführen sind auch jene Datenbearbeitungen, die die Unternehmenseinheit nicht für sich, sondern für andere Unternehmen betreibt bzw. daran beteiligt ist (als Auftragsbearbeiter). Auf jeder Zeile ist daher festzuhalten, ob die angegebene Unternehmenseinheit für die jeweilige Datenbearbeitung **als Verantwortlicher** im Sinne des revidierten DSG und der DSGVO fungiert (→ Glossar) oder "nur" **als Auftragsbearbeiter** (→ Glossar).

- Weiter kann angegeben werden, ob für die betreffende Datenbearbeitung bereits ein **Inventar-Formular** ausgefüllt wurde (d.h. → Formular B.~~1~~2 oder B.~~2~~3), ob ein **Compliance-Check** bereits durchgeführt wurde (d.h. → Formular E.1 oder E.2) und ob eine **Datenschutz-Folgenabschätzung** vorliegt (→ Formular G.1). Ferner kann angegeben werden, ob die Datenbearbeitung unter die DSGVO fällt oder nicht (→ Formular ~~B~~C.1), nebst dem revidierten DSG.

- ~~**Achtung:** Am Ende dieses Formulars finden sich einige Angaben,~~Hinweise, wie die ~~bei der Auswahl der~~ Datenbearbeitungen ~~helfen soll~~ausgewählt werden können, **welche prioritär auf die Einhaltung der Datenschutzvorgaben geprüft** werden sollten, weil sie besonders viele Risiken für betroffene Personen (und das Unternehmen) bergen. Eine solche risikobasierte Vorgehensweise ist üblich.
- Ferner findet sich im Anhang ein optionales **Verzeichnis der Datenschutzerklärungen, Einwilligungen** und weiteren datenschutzrechtlich

Autor: David Rosenthal Alle Rechte vorbehalten. Fachredaktion: David Rosenthal (david.rosenthal@homburger.ch), David Vasella (david.vasella@walderwyss.com)
Dies ist keine Rechtsberatung. Für den Inhalt wird keine Gewähr übernommen. Nutzung auf eigene Gefahr. Lizenz: Creative Commons "Namensnennung – Keine Bearbeitungen 4.0 International"

relevanten Dokumente, die gegenüber betroffenen Personen verwendet werden.

☐ Wir führen diesen Überblick in einer separaten Datei: _____

| | | DB-Nr. | Bezeichnung | Intern zuständig | Verantwort-licher | Auftrags-bearbeiter | Form B.1/2/3 | Form E.1/2 | Form G.1 | DSGVO gilt |
|---|---|---|---|---|---|---|---|---|---|---|
| | | _____ | _____ | _____ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| | | _____ | _____ | _____ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| | | _____ | _____ | _____ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| | | _____ | _____ | _____ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| | | _____ | _____ | _____ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| | | _____ | _____ | _____ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| | | _____ | _____ | _____ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

Eingefüg

Eingefüg

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| | | | | | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| | | | | | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

Weitere Bemerkungen:

**Hinweise zur Priorisierung der Compliance Checks der oben dargestellten Datenbearbeitungen:**

- In B2B-Unternehmen sind die heikelsten Datenbearbeitungen meist jene betreffend die eigenen Mitarbeiter, in B2C-Unternehmen wird oft zunächst auf die Daten der Konsumenten (Kunden) fokussiert, und dort auf die Kernaktivitäten des Unternehmens. Als weniger heikel gelten Daten von Lieferanten und Firmenkunden (auch wenn diese Mitarbeiterdaten enthalten), Daten aus öffentlichen Quellen und Daten, deren Bearbeitung sowieso gesetzlich oder von Dritter Seite genau geregelt ist.

- Folgende Kriterien können helfen, besonders heikle Datenbearbeitungen zu identifizieren. Sind zwei davon gegeben, ist dies unter der DSGVO sogar ein Indiz für ein hohes Risiko, was wiederum eine Datenschutz-Folgenabschätzung verlangt:

  1. Daten werden vertieft analysiert, es findet ein Scoring oder andere Formen des Profiling statt.

  2. Es finden gestützt auf die Daten automatisierte Einzelentscheide statt, die für die betroffene Person rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

  3. Es findet eine systematische Überwachung statt, oder es ist den betroffenen Personen nicht möglich, sich der Datenerhebung zu entziehen.

  4. Es werden besondere Kategorien von Personendaten (→ Glossar) der Daten über strafrechtliche Verurteilungen und Straftaten bearbeitet.

  5. Daten werden in umfangreicher Weise bearbeitet, sei es im Hinblick auf die Zahl der betroffenen Personen, die Datenmenge und Datenvielfalt, die Zeitdauer bzw. Dauerhaftigkeit der Datenbearbeitung, oder örtliche Ausbreitung der Datenbearbeitung.

  6. Es werden verschiedene Datensammlungen und Quellen kombiniert oder aufeinander abgeglichen.

  7. Es werden Daten von besonders schutzbedürftigen Personen wie z.B. Kinder, Arbeitnehmer, Personen mit geistigen Leiden, Asylanten, Patienten, Betagte oder sonst in einem Abhängigkeitsverhältnis stehende Personen bearbeitet.

  8. Es wird im Rahmen der Datenbearbeitung auf innovative Technik oder andere neue Organisationsformen gesetzt, deren negative Folgen bzw. Risiken noch nicht vollends bekannt sind.

  9. Die Datenbearbeitung dient dazu zu bestimmen, wem eine Leistung oder ein Vertrag angeboten werden soll, oder erschwert sonst die Ausübung von Rechten durch die betroffenen Personen.

- Könnte eine Datenbearbeitung in der öffentlichen Wahrnehmung als heikel betrachtet werden oder kann sie für eine betroffene Person nachhaltig gewichtige negative Folgen zeitigen, ob bei korrekter oder missbräuchlicher Durchführung, so sollte diese Datenbearbeitung prioritär beurteilt werden.

**Beispiele für die Datenbearbeitungen eines mittelgrossen Unternehmens (B2C):**

Personalwesen – Personaladministration
Personalwesen – Lohnbuchhaltung
Personalwesen – Rekrutierung
Personalwesen – Sicherheit und Gesundheit
Personalwesen – Schulungsmanagement
Personalwesen – Karriereentwicklung
Marketing & Verkauf – Kundendatenverwaltung
Marketing & Verkauf – Kundenbuchhaltung, Rechnungs- & Zahlungswesen
Marketing & Verkauf – Kundenbindungsprogramm
Marketing & Verkauf – Marketing, Kundenanlässe
Marketing & Verkauf – Kundendienst
Marketing & Verkauf – Online-Shop
Marketing & Verkauf – App
Marketing & Verkauf – Newsletter
Marketing & Verkauf – Marktforschung
Marketing & Verkauf – Produktentwicklung und -tests
Lieferanten & Partner – Lieferantenverwaltung
Lieferanten & Partner – Online-Beschaffungsplattform
Lieferanten & Partner – Händlerverwaltung
Lieferanten & Partner – Promotoren
Lieferanten & Partner – Vertragsmanagement
Finanzverwaltung – Finanz- und Rechnungswesen
Finanzverwaltung – Spesenverwaltung
Finanzverwaltung – Immobilien, Finanzanlagen
Kommunikation – Interne Kommunikation
Kommunikation – Medienstelle
Kommunikation – Website
Logistik & Betrieb – Videoüberwachung
Logistik & Betrieb – Gebäudezugangskontrollen
Logistik & Betrieb – Besucherdatenverwaltung
Logistik & Betrieb – Flottenmanagement
Logistik & Betrieb – Gebäudemanagement
Informatik – Verzeichnisdienste
Informatik – E-Mail-System
Informatik – Dokumentenablage
Informatik – Netzwerküberwachung
Informatik – Geräteverwaltung
Unternehmen – Rechtswesen
Unternehmen – Administration Aktionariat
Unternehmen – Administration Verwaltungsrat und Geschäftsleitung
Unternehmen – Interne Revision
Unternehmen – Interne Untersuchungen

Hinweis: In einem kleinen Unternehmen kann die Aufstellung sehr viel einfacher ausfallen. Es können auch diverse Datenbearbeitungen zusammengefasst werden (z.B. Personalwesen als eine einzige Datenbearbeitung). Eine spezifische gesetzliche Vorgabe gibt es hierzu nicht. Die Flughöhe sollte so gewählt werden, dass sich die diversen weiteren Arbeiten (Inventar, Compliance Check, etc.) sinnvoll beantworten lassen. Oft merkt jemand erst dann, wenn er z.B. Formular E.1 ausfüllt, dass es gescheiter ist ein, zwei Datenbearbeitungen zusammenzufassen oder eine aufzutrennen. Es gibt kein "richtig" oder "falsch".

## Verzeichnis der Datenschutzerklärungen, Einwilligungen und weiteren Datenschutzdokumente (Optional)

Wir setzen gegenwärtig folgende Datenschutzerklärungen (**DSE**) ein:

| Bezeichnung / ID / Anlage | Welcher Bereich wird abgedeckt | Wie kommuniziert? | Wer ist verantwortlich? | DSGVO konform |
|---|---|---|---|---|
| | | | | ☐ |
| | | | | ☐ |
| | | | | ☐ |
| | | | | ☐ |
| | | | | ☐ |
| | | | | ☐ |
| | | | | ☐ |
| | | | | ☐ |
| | | | | ☐ |
| | | | | ☐ |

☐ Wir führen diesen Überblick in einer separaten Datei: _____

Hinweise: Unternehmen haben z.B. oft eine allgemeine DSE ein, eine DSE für die Website und eine DSE für die Bearbeitung von Mitarbeiterdaten. Hinzu können spezielle Erklärungen kommen (z.B. eines Online-Bewerbungssystems). Auch kurze DSE sollten aufgeführt werden, wenn sie eine eigenständige Bedeutung haben. Dokumente, welche lediglich einen Link auf eine Datenschutzerklärung enthalten, sind hier hingegen nicht aufzuführen. Die hier aufgeführten Erklärungen können entweder in der ersten Spalte wahlweise auch mit einer Dokumentenreferenz oder Verweis auf eine Anlage zu diesem Formular aufgeführt werden. Die Frage "Wer ist verantwortlich" meint die interne Verantwortlichkeit für die DSE (der interne "Eigner").

Wir erheben gegenwärtige folgende Einwilligungen:

| Bezeichnung / ID / Anlage | Worin wird eingewilligt? | Wo und wie? | Wer ist verantwortlich? | DSGVO konform |
|---|---|---|---|---|
| | | | | ☐ |
| | | | | ☐ |
| | | | | ☐ |
| | | | | ☐ |
| | | | | ☐ |
| | | | | ☐ |
| | | | | ☐ |
| | | | | ☐ |
| | | | | ☐ |
| | | | | ☐ |
| | | | | ☐ |

☐ Wir führen diesen Überblick in einer separaten Datei: _____

Hinweise: Einwilligungen unterliegen besonderen rechtlichen Anforderungen und können jederzeit zurückgezogen werden, ganz speziell im Rahmen der DSGVO (vgl. Formulare E.3 und E.4). Darum ist es sinnvoll, dass ein Unternehmen weiss, wo es solche Einwilligungen einholt (z.B. auf der Website betr. Anmeldung zum Newsletter, als Checkbox beim Hochladen eines Bewerbungsdossiers, auf einem Papierformular für einen Versicherungsantrag, implizit durch das Ausfüllen eines Formulars) und auf welche Weise (ausdrücklich, implizit [d.h. durch eine Handlung, die Zustimmung impliziert], stillschweigend [d.h. im Stil von "ohne Gegenbericht gehen wir von Ihrer Zustimmung aus]) und in welcher Form (z.B. Website, Papiertalon, mündlich).

Wir haben gegenwärtige folgende weitere datenschutzrechtliche Dokumente, die wir im Verkehr mit betroffenen Personen einsetzen:

| Bezeichnung / ID / Anlage | Art des Dokuments? | Wo und wie? | Wer ist verantwortlich? | DSGVO konform |
|---|---|---|---|---|
| | | | | ☐ |
| | | | | ☐ |
| | | | | ☐ |
| | | | | ☐ |
| | | | | ☐ |
| | | | | ☐ |
| | | | | ☐ |
| | | | | ☐ |
| | | | | ☐ |
| | | | | ☐ |
| | | | | ☐ |

☐ Wir führen diesen Überblick in einer separaten Datei: _____

Hinweise: In dieser Liste sind weitere Dokumente (im weitesten Sinne, d.h. auch Masken auf Websites oder Angaben in Apps) aufzuführen, die in datenschutzrechtlichen Belangen im Verkehr mit betroffenen Personen zum Einsatz kommen, und weder eine DSE, noch eine Einwilligung sind (diese sind oben aufzuführen). Zu denken ist etwa an Standardantworten auf Auskunftsbegehren und sonstige Begehren von betroffenen Personen, Ausführungen zum Datenschutz etwa in Prospekten, Marketingunterlagen, Präsentationen, Handbüchern oder Programmen, nicht durch Datenschutzgesetze motivierte Erklärungen zu Datenbearbeitungen (z.B. Hinweise gemäss Versicherungsvertragsgesetz).