Grundlegende Prinzipien und Begriffsbestimmungen des Datenschutzes finden Sie in Art. 4 und Art. 5 DSGVO.

Schutzziel des Datenschutzes sind nicht (nur) vorhandene Daten, sondern das Informationelle Selbstbestimmungsrecht und die Privatsphäre des Einzelnen. Dies ist ein Grundrecht, verankert in Art. 1 und 2 des Grundgesetzes, der Menschenrechtscharta der EU und dem Menschenrechtskatalog der UN.

Fügen Sie ggf. Einwilligungserklärungsentwürfe, Fragebögen, Projektskizzen, Kooperationsverträge, Auftragsverarbeitungsverträge (AVV) bei.

Rot umrandete Felder sind Pflichtfelder.

Dokumentation einer Verarbeitungstätigkeit

☐ Erstmalige Beschreibung der Verarbeitungstätigkeit

☐ Änderung der Beschreibung vom _____ Datumsformat ist Tag/Monat/Jahr

1. Bezeichnung der Verarbeitungstätigkeit

2. Stand (Datum)

_____ Datumsformat ist Tag/Monat/Jahr

3. Verantwortlicher (Art. 24 DSGVO)

Hochschule für Wirtschaft und Recht Berlin (HWR Berlin)
vertreten durch den Präsidenten Jens Hermsdorf
Badensche Straße 52
10825 Berlin

E-Mail: praesident@hwr-berlin.de

4. Ggf. gemeinsamer Verantwortlicher (Art. 26 DSGVO) außerhalb des Unternehmens (mit Kontaktdaten).

5. Anderer Verantwortlicher in den Fällen, in denen wir die Auftragsverarbeiter sind (sehr selten)

6. Auftragsverarbeiter (Art. 28 DSGVO) mit Kontaktdaten

7.a) Verfahrensverantwortlicher

7.b) Prozessverantwortlicher

8. Datenschutzbeauftragter (Art. 37 und Art. 38 DSGVO)

Klaus Hoogestraat
c/o ITM Management & Consulting GmbH
datenschutzbeauftragter@hwr-berlin.de

9. Zweck der Verarbeitung (Art. 5 Abs. 1 lit. b DSGVO)

10. Rechtsgrundlagen (Art. 6, Art. 9 und Art. 49 DSGVO sowie ggf. ergänzende Regelungen)

Einwilligung (Art. 6 Abs. 1 lit. a)
Vertrag mit Betroffenem (Art. 6 Abs. 1 lit. b)
rechtliche Verpflichtung des Verantwortlichen (Art. 6 Abs. 1 lit. c)
lebenswichtige Interessen (Art. 6 Abs. 1 lit. d)
öffentliches Interesse oder öffentliche Gewalt (Art. 6 Abs. 1 lit. e)
berechtigtes Interesse (Art. 6 Abs. 1 lit. f)
besonders schützenswerte Daten (Art. 9 Abs. 2 lit. a bis j)
Ausnahmen für Übermittlung in Drittländer im Einzelfall (Art. 49 Abs. 1)

11. Kategorien der Betroffenen (Art. 4 Nr.1 DSGVO)

12. Kategorien der personenbezogenen Daten (Art. 4 Nr. 1 DSGVO)

13. Verarbeitungsmittel nach Zweck der Verarbeitung (Art. 32 DSGVO)

14. Kategorien der Empfänger (Art. 4 Nr. 9 DSGVO)

15. Übermittlung in ein Drittland außerhalb des Geltungsbereiches der DSGVO (= EWR)

16. Garantien für eine Übermittlung in ein Drittland (Art. 45 und Art. 46 DSGVO)

17. Beschreibung der Verarbeitungstätigkeit (Was wird gemacht?)

18. Löschfristen mit Beginn

19. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (TOMs) gemäß Art. 32 Abs. 1 DSGVO

Weitere Angaben

Diese Seite wird vom Datenschutzbeauftragten bearbeitet.

20. Datenschutzfolgeabschätzung (Art. 35 DSGVO)

Ist für die Form der Verarbeitung eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO erforderlich?

☐ Ja

☐ Nein

Falls ja, bis wann durchzuführen oder zu überprüfen?

☐ Datumsformat ist Tag/Monat/Jahr

Begründung

21. Stellungnahme des behördlichen Datenschutzbeauftragten

☐ keine Einwände ☐ unter Auflagen ☐ Ablehnung

bei Auflagen oder Ablehnung bitte Erläuterung

1. Bezeichnung der Verarbeitungstätigkeit

Geben Sie hier eine aussagefähige Bezeichnung der Verarbeitungstätigkeit ein.

2. Stand (Datum)

Der Stand der letzten Bearbeitung.

3. Verantwortlicher (Art. 24 DSGVO)

Der Verantwortliche ist die Person oder Organisation, die entscheidet, warum und wie personenbezogene Daten verarbeitet werden – zum Beispiel ein Unternehmen, ein Verein oder eine Behörde.

Nach Artikel 24 der DSGVO muss der Verantwortliche dafür sorgen, dass die Regeln zum Datenschutz eingehalten werden. Dieses gilt auch dann, wenn in seinem Namen Daten durch Dritte verarbeitet werden.

4. Gemeinsamer Verantwortlicher (Art. 26 DSGVO)

Gemeinsam Verantwortliche sind zwei oder mehr Organisationen oder Personen, die zusammen darüber entscheiden, warum und wie personenbezogene Daten verarbeitet werden.

Zum Beispiel:

Wenn zwei Firmen ein gemeinsames Kundenportal betreiben und beide über die Datennutzung entscheiden, sind sie gemeinsam verantwortlich.

Nach Artikel 26 der DSGVO müssen sie klar regeln, wer von beiden wofür zuständig ist – zum Beispiel bei der Information der Betroffenen oder bei der Datensicherheit. Trotzdem können sich Betroffene an jede der beteiligten Stellen wenden.

5. Anderer Verantwortlicher

In Ausnahmefällen kann es sein, dass wir Daten im Auftrag eines Dritten verarbeiten. In diesem Falle ist unser Auftraggeber der Verantwortliche im Sinne der DSGVO.

Sollte dies bei dieser Verarbeitungstätigkeit der Fall sein, geben Sie bitte Name, Adresse und soweit vorhanden eine Vertragsnummer des Auftraggebers ein.

6. Auftragsverarbeiter

Ein Auftragsverarbeiter ist eine Firma oder Person, die im Auftrag eines Verantwortlichen personenbezogene Daten verarbeitet – also nicht für sich selbst, sondern nur nach Anweisung.

Beispiel:

Ein Unternehmen beauftragt einen IT-Dienstleister, Kundendaten zu speichern oder Newsletter zu verschicken. Dann ist der Dienstleister der Auftragsverarbeiter.

Nach Artikel 28 der DSGVO muss der Verantwortliche mit dem Auftragsverarbeiter einen Vertrag abschließen, der den Datenschutz regelt.

7. Verantwortliche Organisationseinheit

Die verantwortliche Organisationseinheit ist die Stelle innerhalb der Organisation, bei der die

personenbezogenen Daten verarbeitet werden und die für den fachlich korrekten Umgang mit diesen Daten verantwortlich ist.

8. Datenschutzbeauftragter

Ein Datenschutzbeauftragter ist eine interne oder externe Person, die darauf achtet, dass ein Unternehmen, eine Behörde oder ein Verein die Datenschutzregeln einhält.

Er oder sie

- berät das Unternehmen zum Datenschutz,
- überwacht die Einhaltung der DSGVO,
- ist Ansprechperson für Mitarbeiter, Betroffene und Aufsichtsbehörden.

Wichtig: Der Datenschutzbeauftragte ist unabhängig und darf keine Nachteile wegen seiner Aufgaben haben.

9. Zweck der Verarbeitung

Der Zweck der Verarbeitung beschreibt, warum personenbezogene Daten überhaupt verarbeitet werden – also zu welchem konkreten Ziel.

Beispiele für Zwecke:

- Eine Bestellung abwickeln.
- Einen Vertrag erfüllen.
- Eine Bewerbung bearbeiten.
- Werbung verschicken (wenn erlaubt)

Nach der DSGVO dürfen Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke verarbeitet werden. Neue Zwecke dürfen nicht einfach dazukommen, ohne die Betroffenen zu informieren.

10. Rechtliche Grundlagen

Seit Einführung der DSGVO gilt der Grundsatz des Verarbeitungsverbotes. D. h., personenbezogene Daten dürfen nicht verarbeitet werden, wenn es keine Rechtsgrundlage gibt.

Die Rechtsgrundlagen sind in verschiedenen Artikeln der DSGVO festgelegt. Grundsätzlich ist es möglich, dass mehrere Rechtsgrundlagen zutreffen. Dieses sollte aber die absolute Ausnahme bleiben, da im Falle eines Rechtstreits die Rangfolge strittig ist.

Die rechtlichen Grundlagen im Einzelnen.

Einwilligung (Art. 6 Abs. 1 lit. a DSGVO)

Die betroffene Person hat ihre Einwilligung zur Verarbeitung gegeben. Dabei ist ist Folgendes zu beachten:

- Die Einwilligung gilt nur für einen bestimmten Zweck. Der Zweck darf ohne erneute Einwilligung nicht verändert oder erweitert werden.
- Die Einwilligung kann jederzeit widerrufen werden. Dem Widerruf ist unverzüglich Folge zu leisten. In der Vergangenheit verarbeitete Daten dürfen weiterhin gespeichert werden, die Daten dürfen aber nicht mehr verarbeitet werden.

- Die Einwilligung muss nachweislich erfolgt sein. Dieses ergibt sich aus der Rechenschaftspflicht der DSGVO. D. h., die Einwilligung muss so dokumentiert sein, dass sie zu einem späteren Zeitpunkt nachgewiesen werden kann.
  Bitte stellen Sie uns bei Einreichung der Verarbeitungstätigkeit einen Entwurf der Einwilligungserklärung zur Verfügung.

Rechtliche Verpflichtung des Verantwortlichen (Art. 6 Abs. 1 lit. b DSGVO)

Der Verantwortliche hat eine Vielzahl von Gesetzen und anderen Rechtsvorschriften einzuhalten. Wenn die Verarbeitung zu Erfüllung derselben erforderlich ist, wählen Sie bitte diese Rechtsgrundlage.

Zur Erfüllung eines Vertrages (Art. 6 Abs. 1 lit. c DSGVO)

Ist die Verarbeitung zur Erfüllung eines Vertrages mit der betroffenen Person erforderlich, z. B. zur Zahlung von Gehalt, Meldungen an Finanzamt oder Krankenkassen, usw., wählen Sie bitte diese Rechtsgrundlage.

Bei lebenswichtigen Interessen (Art. 6 Abs. 1 lit. d DSGVO)

Lebenswichtige Interessen haben Vorrang. Hierzu gehören zum Beispiel die Verarbeitung personenbezogener Daten bei einem Unfall, bei Bränden, usw. Bitte wählen Sie bei einer Verarbeitung in Zusammenhang mit lebenswichtigem Interesse diese Rechtsgrundlage.

Bei öffentlichen Interessen oder öffentlicher Gewalt (Art. 6 Abs. 1 lit. e DSGVO)

Wenn öffentliche Interessen überwiegen oder die Verarbeitung zur Ausübung öffentlicher Gewalt erforderlich ist, wählen Sie bitte diese Rechtsgrundlage.
WICHTIG! Veranstaltungen unterliegen in der Regel NICHT dem öffentlichen Interesse. Bei Veröffentlichungen im Zusammenhang mit Veranstaltungen (z. B. Bildern) sind Einwilligungen einzuholen.

Berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO)

Wenn ein berechtigtes Interesse des Verantwortlichen besteht und keine überwiegenden Interessen oder Rechte der betroffenen Personen entgegenstehen, kann diese Rechtsgrundlage genutzt werden.

WICHTIG! Vor der Verarbeitung ist sorgfältig abzuwägen, ob die eigenen Interessen die Rechte der betroffenen Personen nicht verletzen. Typische Beispiele: Videoüberwachung zur Sicherheit oder Veröffentlichung von Fotos bei Veranstaltungen mit vorherigem Hinweis.

Das berechtigte Interesse und die Ergebnisse der Interessenabwägung sind in jedem Fall zu dokumentieren.

Besonders schützenswerte Daten (Art. 9 Abs. 2 lit. a bis j DSGVO)

Die Verarbeitung besonders sensibler Daten (z. B. zur Gesundheit, Religion oder politischen Meinung) ist grundsätzlich verboten – außer, es greift eine gesetzlich geregelte Ausnahme nach Art. 9 Abs. 2 DSGVO.

Eine Ausnahme liegt nur dann vor, wenn z. B. eine ausdrückliche Einwilligung der betroffenen Person vorliegt, die Verarbeitung aus Gründen des öffentlichen Interesses im Bereich der Gesundheit erfolgt oder gesetzlich vorgeschrieben ist. Im Zweifel fragen Sie bitte den Datenschutzbeauftragten des Verantwortlichen.

Übermittlung in Drittländer im Einzelfall (Art. 49 Abs. 1 DSGVO)

Wenn personenbezogene Daten in ein Land außerhalb der EU übermittelt werden sollen, in dem **kein angemessenes Datenschutzniveau** herrscht, darf dies nur ausnahmsweise auf Grundlage von Art. 49 Abs. 1 DSGVO erfolgen. Ausnahmsweise bedeutet, dass die Einwilligung für jeden Einzelfall einer Übermittlung einzuholen ist.

Diese Ausnahmen greifen nur in besonderen Fällen – z. B. wenn die betroffene Person ausdrücklich eingewilligt hat, die Übermittlung zur Vertragserfüllung erforderlich ist oder ein wichtiges öffentliches Interesse besteht. Solche Fälle sind sorgfältig zu dokumentieren und rechtlich zu prüfen.

11. Kategorien der Betroffenen (Art. 4 Nr. 1 DSGVO)

Betroffene Personen sind Menschen, deren **personenbezogene Daten verarbeitet** werden – also über die Daten gesammelt, gespeichert oder genutzt werden.

Die **Kategorien der Betroffenen** beschreiben, **zu welcher Personengruppe** diese Menschen gehören.

Beispiele für Kategorien:

- **Kunden**
- **Mitarbeitende / Bewerber**
- **Lieferanten / Geschäftspartner**
- **Webseitenbesucher**
- **Patienten**
- **Schüler oder Studierende**

12. Kategorien der personenbezogenen Daten (Art. 4 Nr. 1 DSGVO)

Personenbezogene Daten sind alle Informationen, die sich auf eine **bestimmte oder bestimmbare Person** beziehen – also Daten, mit denen man jemanden **direkt oder indirekt erkennen** kann.

Kategorien personenbezogener Daten sind zum Beispiel:

- **Allgemeine Daten:** Name, Adresse, Telefonnummer
- **Digitale Daten:** IP-Adresse, E-Mail-Adresse, Standortdaten
- **Vertragsdaten:** Kundennummer, Kontodaten, Bestellverlauf
- **Besondere Kategorien** (sensibel):
    - Gesundheitsdaten
    - Daten zur Religion, politischen Meinung oder Gewerkschaft
    - Biometrische Daten (z. B. Fingerabdruck)

Die Kategorien helfen dabei, zu entscheiden, **wie schützenswert** bestimmte Daten sind und **welche Schutzmaßnahmen** nötig sind.

13. Verarbeitungsmittel nach Zweck der Verarbeitung (Art. 32 DSGVO)

Verarbeitungsmittel sind die **technischen und organisatorischen Mittel**, mit denen personenbezogene Daten verarbeitet werden – zum Beispiel Software, Server, Netzwerke oder Verfahren.

Nach **Artikel 32 der DSGVO** müssen diese Verarbeitungsmittel **dem Zweck der Datenverarbeitung angemessen** sein. Das heißt:

Je **sensibler die Daten** und je **größer das Risiko**, desto **stärker müssen die Schutzmaßnahmen** sein.

Typische Verarbeitungsmittel sind:

- Papier
- IT-Anwendungen (z. B. Outlook, Word, Excel, Cloud-Dienste)
- Multifunktionsdrucker

14. Kategorien der Empfänger (Art. 4 Nr. 9 DSGVO)

Empfänger sind Personen, Unternehmen oder Stellen, an die **personenbezogene Daten weitergegeben** werden – egal ob es sich dabei um Dritte oder verbundene Unternehmen handelt.

Die **Kategorien der Empfänger** beschreiben also, **an wen** Daten übermittelt werden können.

Beispiele für Empfänger-Kategorien:

- **Interne Abteilungen** (z. B. Buchhaltung, Personalabteilung)
- **Dienstleister** (z. B. IT-Anbieter, Versanddienstleister, Steuerberater)
- **Behörden** (z. B. Finanzamt, Sozialversicherung)
- **Kooperationspartner**
- **Konzernunternehmen**

15. Übermittlung in ein Drittland außerhalb des Geltungsbereiches der DSGVO (= EWR)

Wenn personenbezogene Daten in ein **Land außerhalb des Europäischen Wirtschaftsraums (EWR)** übermittelt werden, spricht man von einer **Drittlandübermittlung**.

Der **EWR** umfasst:

- alle EU-Staaten
- plus Island, Liechtenstein und Norwegen

Zu den Drittländer gehören u. a.

- USA
- Indien

- China
- viele andere Länder außerhalb Europas

Damit der Datenschutz dort genauso gut ist wie in der EU, muss sichergestellt werden, dass das Drittland **angemessene Schutzmaßnahmen** bietet.

16. Garantien für eine Übermittlung in ein Drittland (Art. 45 und Art. 46 DSGVO)

Wenn personenbezogene Daten in ein **Drittland** (außerhalb des EWR) übermittelt werden, muss sichergestellt sein, dass die Daten dort **genauso gut geschützt** sind wie in der EU.

Daten dürfen nur in Drittländer übermittelt werden, wenn dort **ein angemessenes Datenschutzniveau** herrscht – entweder durch einen **EU-Beschluss** oder durch **spezielle vertragliche Garantien**.

17. Beschreibung der Verarbeitungstätigkeit

Bitte beschreiben sie genau, was mit den personenbezogenen Daten im Rahmen der Verarbeitungstätigkeit gemacht wird.

18. Löschfristen mit Beginn

Die DSGVO fordert die Löschung der Daten, sobald der Zweck erfüllt ist. Das ist in der Regel dann der Fall, wenn gesetzliche Aufbewahrungsfristen erreicht sind. Bitte führen Sie hier die geltenden Aufbewahrungsfristen auf.

Das Recht auf Löschung (Artikel 17 DSGVO) kann i. d. R. erst nach Ablauf von Aufbewahrungsfristen erfüllt werden.

Ausnahmen von dieser Regelung sind mit dem Datenschutzbeauftragten vorab abzustimmen.

19. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 32 Abs. 1 DSGVO)

Technische und organisatorische Maßnahmen (kurz **TOMs**) sind alle Vorkehrungen, die eine Organisation oder eine Behörde treffen muss, um **personenbezogene Daten zu schützen** – z. B. vor Verlust, Diebstahl oder unbefugtem Zugriff.

Die Maßnahmen müssen dem **Risiko angemessen** sein – je sensibler die Daten, desto strenger der Schutz.

Die detaillierte Aufführung von TOMs ist an dieser Stelle nicht erforderlich und auch nicht erwünscht. Bitte verweisen Sie an dieser Stelle lediglich auf ein Dokument, in dem diese beschrieben sind.

Stellen Sie uns dieses Dokument bitte zusammen mit dieser Verarbeitungstätigkeit zur Verfügung, da es wichtig für die lückenlose Dokumentation ist.

20. Datenschutzfolgenabschätzung (Art. 35 DSGVO)

Eine **Datenschutz-Folgenabschätzung** (DSFA) ist eine **Risikoanalyse**, die durchgeführt werden muss, **wenn eine Datenverarbeitung ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen** mit sich bringen könnte.

Ziel ist, Risiken zu erkennen und Schutzmaßnahmen zu planen, **bevor** mit der Datenverarbeitung begonnen wird.

Eine DSFA ist zwingend erforderlich, wenn z. B.

- sensible Daten (z. B. Gesundheitsdaten) verarbeitet werden,
- Personen systematisch überwacht werden (z. B. per Kamera),
- neue Technologien eingesetzt werden (z. B. KI oder Tracking-Systeme),
- große Mengen an Daten auf einmal verarbeitet werden.

Der Datenschutzbeauftragte entscheidet über die Erfordernis einer Datenschutz-Folgenabschätzung und steht Ihnen gerne beratend zur Verfgüung.

21. Stellungnahme des behördlichen Datenschutzbeauftragten

Zum Abschluß seiner Prüfung entscheidet der Datenschutzbeauftragte, ob die Verarbeitung zulässig ist oder nicht. In Ausnahmefällen wird er Auflagen erteilen. Dieses kann z. B. eine Überprüfung der Verarbeitung nach einem bestimmten Zeitraum sein.