Praktische Hilfe zur Umsetzung der DSGVO für Naturparke Deutschland

Diese Anleitung soll Ihnen dabei helfen, sich für die DSGVO zu rüsten.

Inhalt

Anhang

Zu Schritt 2: Verarbeitungsverzeichnis_Muster (Excel-Datei)

Zu Schritt 3: AuftragsverarbeitungsVertrag_Muster (Word-Datei)

Zu Schritt 4:

- a) Verpflichtung-Datengeheimnis (Word-Datei)
- b) Einwilligungserklärung_Mitarbeiter (Word-Datei)
- c) EDV-Richtlinie_Benutzer (Word-Datei)
- d) Datenschutzerklärung-Mitarbeiter (Word-Datei)

Zu Schritt 6:

- a) Anleitung_DSGVO-sichere-Website (PDF-Datei)
- b) Rechtsgrundlage_Einwilligungen-und-Alternativen
- c) Maßnahmen-Dokumentation (Word-Datei)

Zu Schritt 7:

- a) DSGVO-Auskunftsformular_Vorlage (Excel-Datei)
- b) Datenschutz-Logbuch_Vorlage (Excel-Datei)

DIE WICHTIGSTEN BEGRIFFE ZUR DSGVO

Zu Beginn ist es notwendig, dass Sie die wesentlichsten Begriffe zur Datenschutz-Grundverordnung (DSGVO) kennen und verstehen.

Personenbezogene Daten (Personen-Daten)[1]

Personenbezogen sind Daten, wenn sie sich **auf eine (menschliche) Person beziehen** (z. B. Name, Adresse, Geburtsdatum und auch die IP-Adresse) – das heißt, dass man dadurch die Person identifizieren kann.

Datenverarbeitung[2]

Daten verarbeiten heißt praktisch **„ALLES", was mit Daten geschieht** – egal ob elektronisch oder am Papier (z. B. Speichern, bearbeiten, verwenden …[3]). Auch das bloße Ansehen eines Blattes, auf dem Personen-Daten stehen, kann man als „Verarbeitung" sehen.

Betroffene

Der Betroffene ist **die (menschliche) Person,** von der Sie Daten verarbeiten (z. B. Max Mustermann, Maria Musterfrau). Ziel der DSGVO ist es, die (personenbezogenen) Daten dieser betroffenen Person zu schützen.

Verantwortlicher[4]

Verantwortlich ist derjenige, der **entscheidet, was mit den Daten geschieht**. Es ist bei Unternehmen nicht die menschliche Person (außer bei Einzelunternehmen natürlich), sondern immer das Unternehmen bzw. die Organisation.

Auftragsverarbeiter[5]

Der Verantwortliche kann jemanden **beauftragen, Daten für ihn zu verarbeiten** – und zwar einen Auftragsverarbeiter (früher „Dienstleister" genannt). Darauf werden wir in Schritt 3 genauer eingehen.

[1] DSGVO Art. 4.

[2] DSGVO Art. 4.

[3] Vgl. Bitkom 2017: Das Verarbeitungsverzeichnis, S. 20.

[4] DSGVO Art. 4.

[5] DSGVO Art. 4.

DIE 10 GRUNDREGELN DER DSGVO, DIE SIE EINHALTEN MÜSSEN[6]

In der DSGVO gibt es bestimmte Grundregeln (auch Grundsätze, Prinzipien oder Pflichten genannt), die jede Organisation erfüllen muss, wenn sie Personen-Daten verarbeitet. Wir haben die 10 Grundregeln zusammengefasst und stellen Ihnen diese anhand von Fragestellungen kurz vor:

1. Rechtmäßigkeit: *„Dürfen wir alle Daten verarbeiten?“*
   Sie dürfen Daten nur verarbeiten, wenn Sie dafür eine „Rechtsgrundlage“ haben (Details siehe Schritt 2: Verarbeitungsverzeichnis)

2. Glauben und Transparenz: *„Haben wir die betroffenen Personen aufgeklärt?“ (und zwar leicht zugänglich und einfach verständlich - z. B. durch eine Datenschutzerklärung)*

3. Zweckbindung: *„Haben wir aufgeschrieben, wozu wir die Daten verarbeiten?“*

4. Datenminimierung: *„Wir verarbeiten nur so viele Daten wie notwendig?“ (so wenige wie möglich)*

5. Speicherbegrenzung: *„Haben wir Daten gelöscht, die wir nicht mehr brauchen?“*

6. Richtigkeit: *„Sind unsere Daten (soweit wie praktisch möglich) aktuell und richtig?“*

7. Datensicherheit: *„Sind die Daten sicher? (Haben wir angemessene Maßnahmen zur Datensicherheit gesetzt?)“*

8. Wahrung der Betroffenenrechte: *„Stellen wir alle Rechte der betroffenen Personen sicher (von denen wir Daten verarbeiten)?“*

    a. *Informationspflichten*: Haben Sie die betroffenen Personen über die Datenverarbeitungen informiert? (und zwar in klarer, verständlicher, transparenter und leicht zugänglicher Form)

    b. *Auskunftsrecht*: Die betroffene Person hat ein Recht auf Auskunft über ihre personenbezogenen Daten. Das heißt, Sie müssen den Betroffenen innerhalb eines angemessenen Zeitraums (max. 1 Monat) eine Auskunft geben können, welche Daten Sie verarbeiten.

[6] In Anlehnung an Rosenmayr-Klemenz 2018, S. 26ff; vgl. DSGVO Art. 5-20.

c. *Recht auf Berichtigung*: Die Person hat ein Recht, ihre Daten richtigstellen zu lassen. Das bedeutet, Sie müssen die Personen-Daten korrigieren, wenn Sie darauf aufmerksam gemacht werden.

d. *Recht auf Löschung*: Die Person hat ein Recht, ihre Daten löschen zu lassen. Das heißt, Sie müssen die personenbezogenen Daten auf Aufforderung löschen (außer Sie haben z. B. eine gesetzliche Aufbewahrungspflicht)

e. *Recht auf Einschränkung (Sperrung) der Verarbeitung*: Sollte eine Löschung nicht umsetzbar sein, ist die Einschränkung der Datenverarbeitung eine Zwischenstufe, auf die der Betroffene ein Recht hat.

f. *Mitteilungspflicht*: Hat die betroffene Person ihr Recht auf Löschung in Anspruch genommen, trifft Sie eine Mitteilungspflicht. Das bedeutet, dass Sie alle weiteren Verantwortlichen, an die Sie Daten der betroffenen Person weitergegeben haben, über diese Löschung informieren müssen.

g. *Recht auf Datenübertragbarkeit*: Die Person hat ein Recht, ihre Daten zu erhalten (in einem möglichst gängigen Format) und für eigene Zwecke wiederzuverwerten.

h. *Recht auf Widerspruch*: Die Person hat ein Recht, der Datenverarbeitung zu widersprechen. Dann dürfen Sie als Verantwortlicher die Daten der betroffenen Personen nicht weiter verarbeiten (außer Sie haben z. B. eine gesetzliche Verpflichtung dazu). Ein Beispiel wäre der Widerruf bei E-Mail Marketing: Wenn die Person ihre Zustimmung widerruft, dürfen Sie keine Werbe-E-Mails mehr senden.

9. Dokumentationspflicht: *„Haben wir „alles" nachvollziehbar aufgeschrieben?"*
10. Rechenschaftspflicht: *„Können wir jederzeit und rasch nachweisen, dass wir alle Grundregeln einhalten?"*

Nachdem Sie die im Folgenden genannten 7 Schritte umgesetzt haben, sollten Sie alle 10 Grundregeln erfüllen. Wenn Sie eine (oder mehrere) dieser Grundregeln verletzen, riskieren Sie hohe Strafen.

CHECKLISTE FÜR NATURPARKE: DIE DSGVO IN 7 SCHRITTEN ERFÜLLEN

Mit dieser Checkliste erfahren Sie, welche Maßnahmen umzusetzen sind, um die wichtigsten Anforderungen der Datenschutz-Grundverordnung (DSGVO) zu erfüllen. Diese Checkliste ist speziell auf Naturparke ausgerichtet – und so einfach wie möglich gestaltet.

Die Checkliste zeigt Ihnen die wichtigsten sieben Schritte zur praktischen Umsetzung der neuen Datenschutz-Grundverordnung.

1. Beantworten Sie die wichtigsten Grundfragen
2. Erstellen Sie ein Verarbeitungs-Verzeichnis
3. DSGVO-konforme Auftragsverarbeitung umsetzen
4. Personal-Vereinbarungen treffen
5. Risiko prüfen und abschätzen
6. Sicherheits-Maßnahmen umsetzen
7. Die laufende Einhaltung von Datenschutz sicherstellen

Wenn Sie diese sieben Schritte umsetzen, sollten Sie die notwendigen Anforderungen der neuen Datenschutz-Grundverordnung erfüllen, um Abmahnungen und Strafen zu vermeiden.

Schritt 1: Beantworten Sie die wichtigsten Grundfragen

Beantworten Sie zuerst die wichtigsten Grundfragen – die Antworten darauf benötigen Sie dann in den nächsten Schritten wieder.

1. Frage: Welche Personen-Daten verarbeiten Sie?

- Sammeln Sie alles, was Ihnen einfällt.
  (Beispiele: Mitarbeiter, Partner, Newsletter-Kontakte …)

2. Frage: Verarbeiten Sie sensible Daten?

- In der Regel dürften Sie **keine sensiblen Daten verarbeiten**.
- Doch **zur Kontrolle** ist zu prüfen, ob Sie sensible Daten verarbeiten.
  Folgende Daten zählen laut DSGVO als „sensibel“:[7]
  - Rassische oder ethnische Herkunft (z. B. Geburtsland)
  - Religiöse, politische und weltanschauliche Überzeugungen (z. B. Religionsbekenntnis)
  - Gesundheitsdaten (z. B. Krankenstände)
  - Genetische oder biometrische Daten (z. B. Fingerabdruck)
  - Daten zum Sexualleben oder sexueller Orientierung (z. B. Homosexualität)
- Wenn Sie sensible Daten verarbeiten, versuchen Sie dies **möglichst zu vermeiden**.
  Denn ansonsten müssen Sie Einwilligungen sicherstellen, ggf. Risikoabschätzungen durchführen und strengere Datensicherheitsmaßnahmen einhalten.

[7] DSGVO Art. 9, Abs. 1.

3. Frage: Benötigen Sie einen Datenschutz-Beauftragten?

- Ein **Datenschutz-Beauftragter** ist notwendig, wenn Sie **1 oder mehrere** der folgenden Fragen mit „**JA**“ beantworten können:[8]

  a) Sind Sie eine **Behörde / öffentliche Stelle**?
  b) Sind in Ihrer Organisation **mind. 10 Personen** damit beschäftigt, personenbezogene Daten zu verarbeiten?[9]
  c) Ist es Ihre **Kerntätigkeit, sensible Daten umfangreich** zu verarbeiten?
     - „Kerntätigkeit“ heißt (als praktische Faustregel), wenn Sie einen Großteil Ihres Umsatzes / Ihrer Einnahmen daraus erzielen
     - „Sensible Daten“ verarbeiten (Bedeutung siehe 2. Frage Seite 6)
     - „Umfangreich“ heißt in der Regel, wenn viele Personen betroffen sind oder Sie viele Daten verarbeiten
  d) Ist es Ihre **Kerntätigkeit**, Personen umfangreich oder **systematisch** zu **überwachen**? (z. B. Standort-Tracking, Detektive)?

- Sollten Sie einen Datenschutz-Beauftragten benötigen, **finden Sie einen geeigneten Datenschutz-Beauftragten**

  - Wer darf KEIN Datenschutz-Beauftragter sein?
    - Der **Geschäftsführer selbst** darf auf keinen Fall der Datenschutz-Beauftragte sein, weil der Beauftragte möglichst unabhängig sein sollte.
    - Problematisch ist es auch bei **IT-Verantwortlichen** und **Personal-Leitern**, weil es auch hier Interessenskonflikte geben kann. (Es macht ja z. B. wenig Sinn, wenn sich der IT-Verantwortliche selbst kontrolliert, ob er die Datenschutz-Maßnahmen richtig umsetzt).

  - Wer kann Datenschutz-Beauftragter sein?[10]
    - Die Voraussetzung ist ein **Fachwissen über Datenschutz** (das kann man z. B. über eine Ausbildung mit einem Zertifikat nachweisen)
    - Der Datenschutz-Beauftragte sollte möglichst **unabhängig** sein. Seine Aufgaben als Datenschutz-Beauftragter sollten nicht mit anderen Aufgaben „kollidieren“.
    - Es wäre auch eine Möglichkeit, einen **externen Datenschutz-Experten** zu beauftragen, die Aufgabe als Datenschutz-Beauftragter zu übernehmen.

[8] Vgl. DSGVO Art. 37.

[9] BDSG, Kap. 3, § 38: *„(1) Ergänzend zu Artikel 37 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679 benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen*. […]“

[10] Mehr Infos über die Mindestanforderungen an einen Datenschutzbeauftragten sind zu finden unter: https://www.lda.bayern.de/media/dk_mindestanforderungen_dsb.pdf

Schritt 2: Erstellen Sie ein Verarbeitungs-Verzeichnis

Das Verarbeitungs-Verzeichnis ist die wohl **wichtigste Aufgabe**, die praktisch **JEDE Organisation** machen muss. Es gibt so gut wie **keine Ausnahmen**!

Im Verarbeitungsverzeichnis dokumentieren Sie alle Ihre Daten-Verarbeitungen. Darin schreiben Sie auf, welche Daten Sie wozu verarbeiten, an wen Sie die Daten weitergeben, wie lange Sie diese speichern, warum Sie diese überhaupt verarbeiten dürfen usw.

- **Verwenden Sie bestehende Muster und Vorlagen** von Datenschutz-Vereinen, Kammern oder Experten und passen Sie diese auf Ihre Organisation an.
  Beispiele für Muster:
  - Unser Muster im Anhang als Excel-Vorlage – siehe Anhang 2
  - Ein generelles Muster für Vereine wie beispielsweise vom LDA: *https://www.lda.bayern.de/media/muster_1_verein_verzeichnis.pdf*
  - Oder eine andere Vorlage Ihrer Wahl wie z. B.:
    - Bitkom: *https://www.bitkom.org/Bitkom/Publikationen/Das-Verarbeitungsverzeichnis.html*
    - GDD: https://www.gdd.de/downloads/praxishilfen/Muster_VVT.docx

- Wenn Sie **unsere Excel-Vorlage im Anhang nutzen** (die wir für Sie bereits vorausgefüllt haben), sind folgende Spalten von Ihnen fertigzustellen (richtigstellen und ergänzen):

1. **Betroffene:** Wer sind die betroffenen Personen (zusammengefasst in Kategorien), von denen Sie die Daten verarbeiten? (z. B. Mitarbeiter, Bewerber, Interessenten, …)

2. **Zwecke:** Wozu verarbeiten Sie die Daten? (z. B. Gehaltsabrechnung, Bewerbungs-Bearbeitung, Marketing, Anfrage-Bearbeitung, Newsletter-Versand, …)

3. **Daten-Kategorien:** Welche Daten verarbeiten Sie? (z. B. Stammdaten wie Name und Adresse, Kontaktdaten wie E-Mail und Tel-Nr., Bankdaten, Bilder, …)

4. **Empfänger:** Wohin gehen die Daten / wer bekommt die Daten? (z. B. Steuerberater, Banken, Versicherungen, Partner x, Auftragsverarbeiter y, …)

5. **Fristen:** Wie lange dürfen Sie die Daten aufbewahren? Sie dürfen Daten nur so lange speichern wie nötig.
   a. Wenn möglich, können Sie eine gesetzliche Frist verwenden wie z. B. Personalakten 3 Jahre nach Beschäftigungs-Ende[11], Geschäftsunterlagen 10 Jahre (teilweise 6 Jahre)[12], Bewerberdaten 2-3 Monate[13], Schadensersatz: bis 30 Jahre[14]

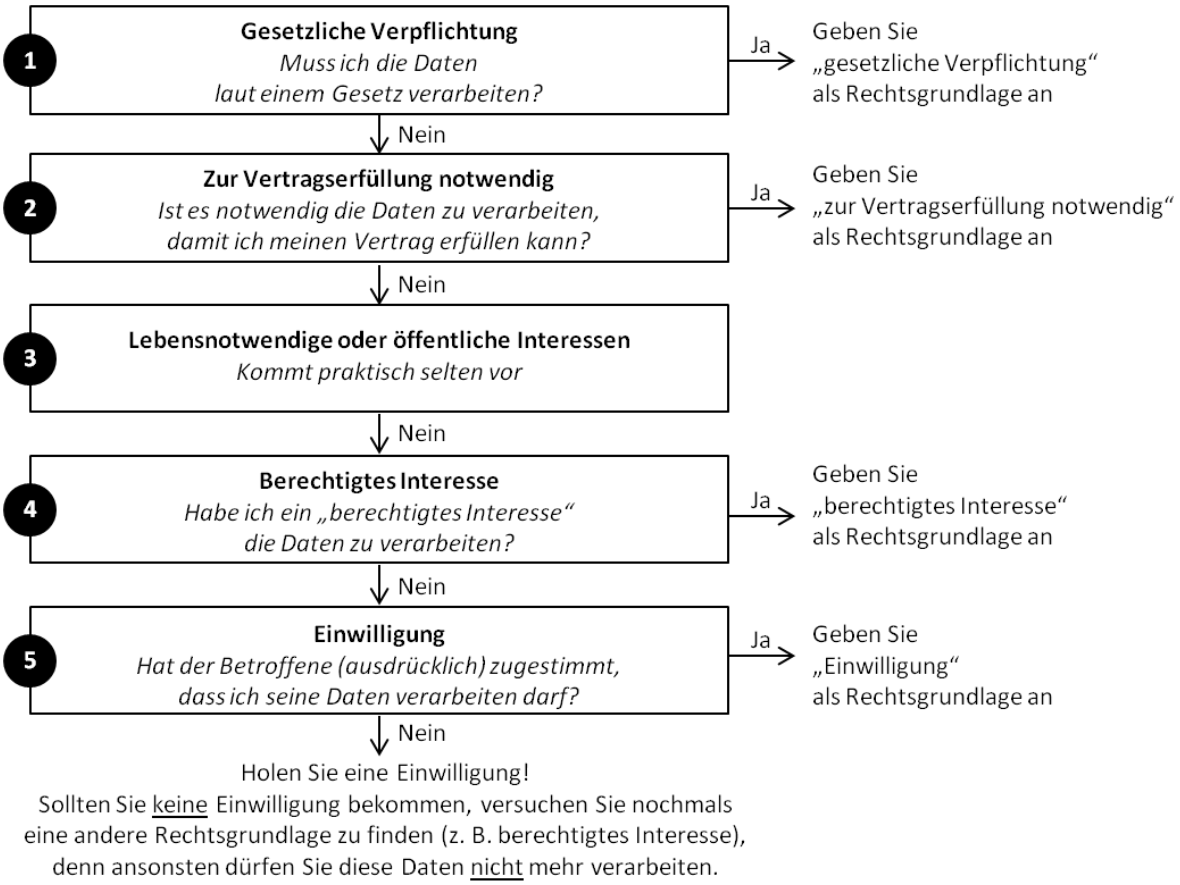
[11] Vgl. https://www.focus.de/finanzen/experten/thies/aufbewahrungspflichten-von-personalakten-fristen-im-ueberblick_id_8203687.html.

[12] Vgl. https://www.hk24.de/produktmarken/beratung-service/recht_und_steuern/steuerrecht/abgabenrecht/aufbewahrungsfristen-geschaeftsunterlagen/1157174#titleInText2

[13] Vgl. https://www.haufe.de/compliance/management-praxis/aufbewahrung-wie-lange-duerfen-bewerberdaten-gespeichert-werden_230130_261218.html: Als gerechtfertigte Aufbewahrungsfrist wird ca. 3 Monate genannt.

b. Ansonsten sollten Sie eine möglichst kurze nachvollziehbare Aufbewahrungsfrist verwenden, sodass Sie die Daten nur so lange speichern, wie Sie diese brauchen.

6. **Rechtsgrundlage:**[15] Dürfen Sie die Daten überhaupt verarbeiten? Warum?
Stellen Sie dabei folgende Fragen (Sie müssen **EINE der Fragen** mit „**Ja**" beantworten):
Bevor Sie Einwilligungen einholen, prüfen Sie jedes Mal folgende Checkliste (und zwar in folgender Reihenfolge von 1 bis 5) – siehe auch Anlage 6b:



➤ **Tipps zur Umsetzung** des Verarbeitungsverzeichnisses:

- Gehen Sie die Excel-Tabelle Zeile-für-Zeile durch und passen Sie diese auf Ihre Organisation an. (Verlieren Sie sich nicht zu sehr im Detail!)
- Versuchen Sie möglichst alles begründen zu können (z. B. warum Sie die Daten für eine bestimmte Zeit speichern und notieren Sie dies jeweils kurz)
- Speichern Sie das Verarbeitungsverzeichnis jeweils als neue Datei mit heutigem Datum ab, damit Änderungen nachvollziehbar bleiben.

[14] Vgl. § 199 Absatz 2 BGB; https://www.advocado.de/ratgeber/vertragsrecht/schadensersatz/verjaehrung-schadensersatz.html.

[15] Vgl. DSGVO, Art. 6.

Schritt 3: DSGVO-konforme Auftragsverarbeitung umsetzen

a) Welche Auftragsverarbeiter haben Sie?

➤ Listen Sie alle Ihre Auftragsverarbeiter auf.

Beispiele für Auftragsverarbeiter[16]	KEIN Auftragsverarbeiter
• IT-Dienstleister (z. B. EDV-Wartung, außer ein Zugriff auf Personen-Daten ist nicht möglich bzw. absolut ausgeschlossen) • Cloud-Anbieter (z. B. für CRM-Lösungen, Online-Buchhaltung) • Webhoster (wenn Sie eine Website haben) • E-Mail Anbieter • Externe Druckdienstleister • Datenvernichtung oder -archivierung • Häufig Google (wenn Sie Google-Dienste nutzen wie z. B. Google Analytics, Adwords, Gmail, GSuite …) • Evtl. Facebook (schwer zum Zuordnen) • …	• Steuerberater und Wirtschaftsprüfer • Rechtsanwälte • Banken • Versicherungen • Postdienstleistungen • Telekommunikationsdienstleistungen • Reiner Datenspeicher, auf dem die Daten verschlüsselt gespeichert sind (z. B. Backup-Cloud-Anbieter ohne weitere Services) • IT-Dienstleister ohne Daten-Verarbeitung (z. B. EDV-Wartung, wenn ein Zugriff auf Personen-Daten ausgeschlossen ist) • …

b) Gibt es Verträge mit Ihren Auftragsverarbeitern?

➤ **Fragen Sie beim Dienstleister nach**, ob er einen „Auftragsverarbeitungs-Vertrag“ zur Verfügung stellt *(Hinweis: Bei Google & Co. gibt es in der Regel aktualisierte Nutzungsverträge/-bedingungen, denen zuzustimmen ist).*

➤ **Verwenden Sie ansonsten Muster**, passen Sie diese für Sie an und schicken Sie den Vertrag an Ihre Dienstleister zur Unterzeichnung

- Unser vereinfachtes Muster im Anhang 3
- Oder eine andere Vorlage wie z. B.
  - GDD: *https://www.gdd.de/aktuelles/startseite/news/neues-gdd-muster-zur-auftragsdatenverarbeitung-gemas-a7-11-bdsg*
  - Bitkom: *https://www.bitkom.org/Bitkom/Publikationen/Begleitende-Hinweise-zu-der-Anlage-Auftragsverarbeitung.html*

➤ **WICHTIG: Stellen Sie sicher, dass Sie mit allen Ihren Auftragsverarbeitern einen Vertrag haben, der den Datenschutz (laut DSGVO) regelt**

c) Sind Sie selbst Auftragsverarbeiter (für jemand anderen)?

➤ **Wenn ja: Erstellen Sie ein Verarbeitungsverzeichnis** für alle Daten, die Sie im Auftrag des Verantwortlichen verarbeiten.

➤ **Wenn nein: Gehen Sie weiter zu Schritt 4.**

[16] Vgl. Bitkom 2017: Begleitende Hinweise zu der Anlage Auftragsverarbeitung, S. 17-23; sowie teilweise https://www.wko.at/service/unternehmensfuehrung-finanzierung-foerderungen/eu-dsgvo-auftragsverarbeiter-faq.html, Stand: 11.04.2018.

Schritt 4: Personal-Vereinbarungen treffen

Wenn Sie Mitarbeiter beschäftigen, sind folgende Maßnahmen zu treffen:
(Sollten Sie keine Mitarbeiter haben, gehen Sie weiter zu Schritt 5).

- **Erstellen Sie folgende Personal-Vereinbarungen für Datenschutz (verpflichtend!):**
  - **Datengeheimnis-Verpflichtungserklärung** – siehe Anhang 4a
    oder z. B. *https://www.qdd.de/aktuelles/startseite/verpflichtung-auf-die-vertraulichkeit*
  - **Schriftliche Einwilligungen**, wenn Sie Mitarbeiter-Daten verarbeiten, die rechtlich nicht unbedingt notwendig sind (z. B. für die Veröffentlichung von Mitarbeiter-Bildern auf der Website) – siehe Anhang 4b
    Orientierungshilfen zur Formulierung siehe z. B. auch:
    https://www.lda.bayern.de/media/oh_einwilligung.pdf
- Wir **empfehlen** Ihnen auch eine EDV-Richtlinie und eine Mitarbeiter-Datenschutzerklärung zu erstellen:
  - **EDV-Richtlinie** (Nutzungsregeln für PC, Smartphone, Telefon usw.) – siehe Anhang 4c
    oder z. B. EDV-Richtlinie für Benutzer des BSI:
    https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/hilfmi/muster/musterrichtlinien/musterrichtlinien.html
  - **Datenschutzerklärung für Mitarbeiter** – siehe Anhang 4d
    oder z. B. *www.wko.at/service/wirtschaftsrecht-gewerberecht/dsgvo-muster-datenschutzerklaerung-mitarbeiter.html*
- Gleichen Sie die Infos der oben genannten Personal-Vereinbarungen mit dem Verarbeitungs-Verzeichnis ab.
- Lassen Sie die oben genannten Personal-Vereinbarungen im Rahmen von Gesprächen und Schulungen von allen Mitarbeitern **unterschreiben.**

Schritt 5: Risiko prüfen und abschätzen

a) Benötigen Sie eine Risikoabschätzung? (Datenschutz-Folgeabschätzung)

- **Eine Risikoabschätzung ist in der Regel nicht notwendig.**

- Zur Sicherheit können Sie folgende **Kontrollfragen** durchgehen, um zu prüfen, ob Sie eine Risikoabschätzung benötigen:
  - Sie müssen nur eine Risikoabschätzung machen, wenn Ihre Datenverarbeitung ein hohes Risiko für die betroffenen Personen darstellt. Häufige Beispiele für ein hohes Risiko sind:[17]
    - Haben Sie eine **Videoüberwachung**?
    - Machen Sie **Profiling**? Das heißt, dass Sie Profile von Personen erstellen (z. B. über ihr Verhalten, für Marketing, durch Web-Analyse-Tools)
    - Verarbeiten Sie **sensible Daten** oder andere **vertrauliche Daten** (z. B. Bankdaten, Standortdaten, Strafdaten, private Kommunikationsdaten …) in „**umfangreicher Art und Weise**“ (viele Personen oder viele Daten …)?
    - Übermitteln Sie (sensible/vertrauliche) Daten in **Drittstaaten** (außerhalb EU)?
    - Verwenden Sie **neue Technologien**, die ein hohes Risiko für die betroffenen Personen darstellen können? (z. B. CRM-Cloud-Lösungen für Kunden)
  - **Tipp**: Achten Sie in nächster Zukunft auf die Veröffentlichung von Listen der Datenschutz-Behörde, in denen sie konkret angibt, bei welchen Fällen eine Risikoabschätzung durchzuführen ist (*Blacklist*) und wann keine notwendig ist (*Whitelist*).

- Falls notwendig, führen Sie in folgenden Schritten eine Risikoabschätzung durch:[18]
  - Beschreiben Sie die Datenverarbeitungen genauer
    - Verwenden Sie das Verarbeitungsverzeichnis als Grundlage
    - Genauere Beschreibung der Abläufe, wie Sie die Daten verarbeiten
    - Welche IT-Systeme und andere Mittel Sie dabei einsetzen
  - Risikoanalyse: Bestimmen und bewerten Sie das Risiko für die Betroffenen
  - Setzen Sie Maßnahmen, um das Risiko zu vermindern
  - Prüfen und erklären Sie, ob Sie das Risiko ausreichend senken konnten.
    Falls trotz aller möglichen Maßnahmen immer noch ein hohes Risiko besteht, müssen Sie dies der Datenschutz-Behörde mitteilen (=vorherige Konsultation), die dann über die weitere Datenverarbeitung entscheidet. (Diese Situation sollten Sie vermeiden.)

[17] Die Datenschutz-Behörde wird eine Blacklist und eine Whitelist veröffentlichen, auf denen sie auflistet, wann eine Risikoanalyse notwendig ist und wann nicht. Doch derzeit ist noch unklar, wann diese Listen veröffentlicht werden; Bitkom: Risk Assessment & Datenschutz-Folgenabschätzung – Leitfaden, 2017, S. 50.

[18] In Anlehnung an Bitkom: Risk Assessment & Datenschutz-Folgeabschätzung – Leitfaden, 2017, ab. S. 38.

Schritt 6: Sicherheits-Maßnahmen umsetzen

- **Stellen Sie sicher, dass Sie alle Basis-Maßnahmen zum Datenschutz umsetzen**. Folgende Schritte sind z. B. für die meisten Vereine und Kleinunternehmen unbedingt nötig:
  - **Löschregeln** festlegen: Löschfristen einhalten und Daten sicher löschen (z. B. Papier in den Shredder, alte CDs oder Festplatten vernichten)
  - **Daten** auf den aktuellsten Stand bringen (z. B. Kundendaten) und nicht mehr benötigte Daten löschen (wie im Verarbeitungsverzeichnis festgelegt).
  - **Sichere Passwörter** verwenden (bei Software, PC-Benutzerkonten, mobilen Geräten …)
  - **Verschlüsselung** einsetzen (Verschlüsselung von Smartphones und USB-Sticks, TLS bei E-Mails usw. Vor allem beim Versand vertraulicher oder sensibler Daten ist eine starke Verschlüsselung wichtig – z. B. Dateien mit 7-Zip per AES256 verschlüsseln)
  - **Sichere Software und Webservices nutzen** (z. B. anstatt kostenloser Webdienste kostenpflichtige Business-Versionen nutzen, die gewähren, dass sie die Anforderungen der DSGVO einhalten.)
  - Stets die **Software aktualisieren** (z. B. Virenschutz, Internetbrowser …)
  - **Datensicherung** (Backups) regelmäßig durchführen, Notfälle testen und Sicherungskopien auch an anderem Ort aufbewahren
  - **WLAN** absichern (starke Verschlüsselung, Passwörter usw.)
  - **Räumliche** Maßnahmen prüfen (z. B. Zutrittskontrolle, Brandschutz usw.)
  - **Clear Desk**: Schreibtisch leeren (nichts herumliegen lassen) und Bildschirm sperren (sobald Sie den PC verlassen)
  - **Weitere Maßnahmen** finden Sie z. B. im Sicherheitshandbuch, das Sie unter folgendem Link herunterladen können: *https://www.wko.at/site/it-safe/sicherheitshandbuch.html*

- **Setzen Sie die wichtigsten Website-Maßnahmen um** wie z.B.:
  - Erstellen Sie eine **Datenschutzerklärung**: Tipp: Verwenden Sie Muster oder Generatoren von spezialisierten Rechtsanwälten.
  - **Veröffentlichen** Sie die Datenschutzerklärung als eigene Seite auf Ihrer Website (nicht unter dem Impressum / den AGB, sondern wirklich eine eigene Seite)
  - **Informieren** Sie die Betroffenen über Ihre Datenschutzerklärung (z. B. Link in E-Mail Signatur usw.).
  - Integrieren Sie auf Ihrer Website einen **Hinweis-Banner** für Ihre Datenschutzerklärung und die Verwendung von Cookies
  - Stellen Sie **Einwilligungen** sicher (z. B. eindeutige Zustimmung für E-Mail Versand, …)
  - **Verschlüsseln** Sie Ihre Website („https“ statt „http“)
  - **Wie Sie Ihre Website und Ihr Online-Marketing (Google, Facebook, Newsletter etc.) für die DSGVO vorbereiten**, haben wir im Anhang 6a genauer zusammengefasst.

- **Prüfen Sie, ob Sie alle 10 DSGVO-Grundregeln einhalten.** Falls Sie noch nicht alle Grundregeln einhalten, setzen Sie weitere Maßnahmen um.
  - Eine Herausforderung ist häufig das Thema „Rechtsmäßigkeit / Einwilligungen“. Daher haben wir im Anhang 6b detailliert zusammengefasst, wie Sie die „richtige“ Rechtsgrundlage festlegen und Einwilligungen sicherstellen.

- **Dokumentieren Sie alle Ihre Maßnahmen** - eine **Vorlage für die Dokumentation Ihrer Datenschutz-Maßnahmen** finden Sie im Anhang 6c.

Schritt 7:
Die laufende Einhaltung von Datenschutz sicherstellen

Bitte bedenken Sie: Datenschutz ist keine einmalige Aufgabe ist, sondern eine regelmäßige Arbeit, die immer mitlaufen sollte (z. B. genauso wie Steuern zahlen oder die Buchhaltung erledigen). Folgende Aufgaben sollten Sie jedenfalls regelmäßig durchführen:

- Die **Datenschutz-Grundsätze** langfristig einhalten und jederzeit bereit sein dies zu **beweisen** *(Achtung: Sie müssen der Datenschutz-Behörde jederzeit nachweisen können, dass Sie alle Datenschutz-Grundsätze einhalten)*
  - Legen Sie fest, wer in Ihrer Organisation **Datenschutz-Ansprechpartner** ist.
  - Beantworten Sie alle Anfragen von betroffenen Personen fristgerecht (innerhalb 1 Monats) – Muster für ein **Auskunftsformular** siehe Anhang 7a
  - Führen Sie ein „**Logbuch**“, in dem Sie alle Anfragen/Widerrufe von betroffenen Personen aufzeichnen und die Erledigung markieren – Muster siehe Anhang 7b
- Ihr **Daten-Verarbeitungsverzeichnis** laufend aktualisieren und erweitern
- Ihre **Auftragsverarbeiter** prüfen (Eine Kontrolle ist zwar nicht vorgeschrieben, doch eine regelmäßige Prüfung ist ratsam, weil auch Sie für Datenschutz-Verletzungen Ihres Auftragsverarbeiters voll haften.)
- Ihr **Personal** regelmäßig schulen und auf dem aktuellsten Stand halten
- Regelmäßig prüfen, ob **Risikoabschätzungen** notwendig (siehe Whitelist und Blacklist, die von der Datenschutz-Behörde veröffentlicht werden) und ggf. aktuell sind
- Ihre **Datenschutz-Maßnahmen** regelmäßig checken und verbessern (Audits) sowie Ihre Maßnahmen-Dokumentation auf dem aktuellen Stand halten:
  - Sind die Maßnahmen wirksam / werden sie umgesetzt?
  - Entsprechen die Maßnahmen dem aktuellen Stand der Technik?
  - Gibt es rechtliche Änderungen? (z. B. Verordnungen, Urteile …)
- Bei Bedarf mit der **Datenschutz-Behörde** „zusammenarbeiten“:
  - Bei einem Datenschutz-Verstoß („Datenpanne“) müssen Sie der Behörde (Aufsichtsbehörde) innerhalb von 72 Stunden eine Meldung machen (Kontakt siehe: *https://www.bfdi.bund.de/DE/Service/Kontakt/kontakt_node.html*).
    Bereiten Sie deshalb frühzeitig eine Meldung an die Datenschutzbehörde vor („Data Breach Notification“). Mehr Infos dazu z. B. unter: *https://www.lda.bayern.de/media/baylda_ds-gvo_8_data_breach_notification.pdf*
  - Speichern Sie alle Datenschutz-Dokumente nachvollziehbar in einem Ordner ab, damit Sie diese stets rasch zur Verfügung haben (wenn die Behörde Unterlagen einfordert).

Impressum

DI Rico Kogleck (geprüfter Datenschutzexperte und Unternehmensberater)
Feldweg 29, A-9400 Wolfsberg
E-Mail: rico@digitalerfolgreich.com

Im Auftrag des VDN – Verband Deutscher Naturparke e.V.
Holbeinstr. 12, D-53175 Bonn
E-Mail: info@naturparke.de

Hinweis

Dieses Dokument basiert auf den Erfahrungen beim Verband der Naturparke Österreichs (VNÖ) und wurde auf die deutschen Naturparke angepasst.

Disclaimer

Sämtliche Inhalte wurden mit größtmöglicher Sorgfalt zusammengestellt, erfolgen jedoch ohne Gewähr. Sie stellen keine Beratungsleistung welcher Art auch immer dar und können eine entsprechende Beratung nicht ersetzen. Insbesondere deswegen wird keine Haftung hinsichtlich Richtigkeit, Vollständigkeit und Aktualität der Informationen (einschließlich des Verweises auf andere Quellen) übernommen. Der Verfasser schließt jegliche Haftung aus, sei es aus Vertrag, Delikt (inklusive Fahrlässigkeit) und/oder jeder anderen Rechtsgrundlage, für Verluste oder Schäden, einschließlich entgangenen Gewinns oder sonstiger direkter oder indirekter Folgeschäden, welche durch den Gebrauch oder das Vertrauen in die in dieser Unterlage zur Verfügung gestellten Informationen oder einer etwaigen Nichtberücksichtigung bestimmter Informationen entstehen.