Checkliste für nDSG und DSV

Inklusive Erklärung und Vorlagen / Beispielen

Inhalt

1. Checkliste

Nr.	Thema / Frage	Ja/Nein
1	Dateninventar vorhanden?	
2	Bearbeitungsverzeichnis nötig? (Für KMU sehr selten) Schweiz: optional / DSGVO: obligatorisch	
3	Auftragsbearbeitungsvertrag vorhanden?	
4	Werden Daten ins Ausland exportiert?	
4.1	Sind unsichere Drittstaaten dabei? (USA)	
4.2	Standarddatenschutzklausel (SCC) vorhanden?	
5	TIA Transfer Impact Assessment vorhanden?	
6	Datenschutzerklärung vorhanden?	
6.1	Datenschutzerklärung ist aktueller als 12 Monate?	
7	Gibt es einen Datenschutzberater?	
8	Ist ein Ablaufplan für Anfragen vorhanden? (Datenausgabe, Löschung, etc.)	
8.1	Wird die Identität des Antragstellers geprüft?	
9	Ablaufplan für Datenpannen vorhanden? (Informationspflicht an betroffene Personen und je nach Fall an EDÖB)	
10	Sind die Mitarbeiter für den Datenschutz geschult?	
11	Ist Google Analytics im Einsatz?	
11.1	Ist ein entsprechendes Consent Banner vorhanden? (Cookie Banner)	
12	Notfallplan bei „Abmahnung“ vorhanden?	
13	Werden Newsletter angeboten?	
13.1	Wird darüber korrekt informiert?	
13.2	Ist Double Opt-in Pflicht?	
13.3	Ist ein Opt-out vorhanden?	
14.	Gibt es anderen E-Mail-Versand?	
14.1	Handelt es sich dabei um Werbung?	
15	Werden Mails per Drittanbieter versendet?	
16	Gibt es Verlinkungen auf Drittseiten?	
16.1	Handelt es sich dabei um Social Media?	

2. Erklärungen

2.1 Was ist ein Dateninventar?

Ein Dateninventar ist eine Auflistung aller im Unternehmen vorhandenen Daten. Dabei steht keine möglichst detailreiche Auflistung im Vordergrund, sondern der einfache und schnelle Überblick welche Daten wo gespeichert werden.
Um dies zu erreichen, reicht eine einfache Tabelle vollständig aus. Wichtig dabei ist, diese aktuell zu halten.

Ein Dateninventar ist NICHT vorgeschrieben, weder im nDSG/DSV der Schweiz noch in der DSGVO. Es bildet jedoch den ersten Schritt zur Erstellung eines Bearbeitungsverzeichnisses. Ändert sich etwas am Dateninventar, muss sehr wahrscheinlich auch das Bearbeitungsverzeichnis angepasst werden.

2.2 Was ist ein Bearbeitungsverzeichnis?

Das Bearbeitungsverzeichnis zeigt auf welche Personendaten wofür, wie und wo bearbeitet werden. Bei einer Bearbeitung müssen die Daten nicht zwingend verändert werden. Es reicht, wenn Daten genutzt werden, damit der Schritt in das Bearbeitungsverzeichnis integriert werden muss. Auch hier befindet sich nicht der Detailgrad im Fokus, sondern die Übersichtlichkeit und Vollständigkeit.

2.2.1 Was sind Personendaten?

Als Personendaten gelten alle Daten, welche einer Person zugeordnet werden können. Darunter fallen offensichtliche Angaben wie Name und Geburtsdatum aber auch IP-Adresse oder das Autokennzeichen.
Ein besonderer Punkt bei den Personendaten sind die «besonders schützenswerten Personendaten». Diese werden im nDSG folgendermassen definiert:

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;

2.2.2 Wann ist ein Bearbeitungsverzeichnis Pflicht?

Nach nDSG ist das Bearbeitungsverzeichnis Pflicht bei Unternehmen mit mehr als 250 Mitarbeitern oder wenn besonders schützenswerten Personendaten bearbeitet werden. Damit ist der Pflichtfall eher die Ausnahme als die Regel.
Auch die DSGVO kennt eine Ausnahme für Unternehmen mit weniger als 250 Mitarbeitern. Hier kommt jedoch der Zusatz, dass die Bearbeitung nur gelegentlich erfolgen darf. Dadurch wird ein Bearbeitungsverzeichnis fast immer Pflicht, wenn die DSGVO für das Unternehmen relevant ist.

Achtung!
1. In der Schweiz wird von einem Bearbeitungsverzeichnis gesprochen, in der EU von einem Verarbeitungsverzeichnis. Inhaltlich handelt es sich um das gleiche Dokument.

2. Auch wenn das Bearbeitungsverzeichnis keine Pflicht ist, gilt es als wichtige Dokumentation und Basis zur Umsetzung von Datenschutzrichtlinien. Gerade für die Auskunfts- und Informationspflicht kann es eine Hilfe sein.

2.3 Was ist ein Auftragsbearbeitungsvertrag?

Auch hier gibt es einen schriftlichen Unterschied zwischen Schweiz und EU, Auftragsbearbeitungsvertrag (CH) und Auftragsverarbeitungsvertrag (EU). Oft wird jedoch der internationale Begriff *Data Processing Agreement* oder DPA genutzt.

Das Ziel ist die Absicherung von Outsourcing bei der Datenbearbeitung. Diese Datenübergabe zur Bearbeitung muss vertraglich geregelt sein.

2.3.1 Ist ein Auftragsbearbeitungsvertrag Pflicht?

Ja, bereits nach altem DSG ist eine Vereinbarung Pflicht. Mit dem nDSG ändert sich inhaltlich wenig, das Fehlen eines Auftragsbearbeitungsvertrag kann neu jedoch gebüsst werden (Busse bis 250'000 CHF).

Ein DPA wird immer benötigt, wenn Daten weitergegeben werden. Unter Bearbeitung wird hier auch die Datensicherung oder das Hosting verstanden.
Die einfache Faustregel ist daher: Werden Daten an ein anderes Unternehmen gesendet, wird ein DPA benötigt.

2.3.2 Wie kommt man an einen Auftragsbearbeitungsvertrag?

Dies ist je nach Firma unterschiedlich. Einige Unternehmen bieten diesen Standardmässig an, andere zeigen diesen nur bei Nachfrage über den Support. Kleinere, lokale Unternehmen ausserhalb Europas werden wahrscheinlich keinen entsprechenden Auftragsbearbeitungsvertrag vorbereitet haben. Hier müsste eine individuelle Lösung ausgearbeitet werden.

2.4 Daten im Ausland

2.4.1 Was sind unsichere Drittstaaten?

Grundsätzlich ist jeder Staat, welcher nicht als sicher eingestuft wird, unsicher. Eine Liste gibt es unter: https://www.fedlex.admin.ch/eli/cc/2022/568/de#annex_1

Als Faustregel kann man sich jedoch merken, alles ausserhalb des EU-Raums gilt tendenziell als unsicher.

2.4.2 Die Standarddatenschutzklauseln

Werden Daten zur Bearbeitung weitergegeben, so bleibt die Haftung trotzdem bestehen. Um sich hier abzusichern wird eine Standarddatenschutzklausel benötigt. Oft wird auch von Standard Contractual Clauses (SCC) gesprochen.

Die Standarddatenschutzklauseln sind in der DSGVO bereits Pflicht, mit dem nDSG werden sie es auch für die Schweiz.

Die SCC sind je nach Unternehmen ein Teil des Auftragsbearbeitungsvertrag oder der ABG.

2.5 Transfer Impact Assessment vorhanden?

Das Transfer Impact Assessment (TIA) dient als Risikoeinschätzung bei der Datenbearbeitung bei Dritten im Ausland.
Es wird geprüft, ob der Datenbearbeiter aufgrund lokaler Vorschriften gezwungen sein kann, gegen die Regelungen in den SCC zu verstossen. Das Ergebnis dieser Prüfung muss dokumentieren werden.

2.5.1 Ist das Transfer Impact Assessment Pflicht?

Das TIA ist nach nDSG keine Pflicht, jedoch wird es empfohlen. In der DSGVO ist es keine direkte Pflicht, leitet sich aber als Pflicht aus der SCC ab. Werden die Standarddatenschutzklauseln der EU genutzt, muss auch ein TIA erstellt werden.

2.6 Datenschutzerklärung vorhanden?

Die Datenschutzerklärung wird sowohl vom aktuellen DSG als auch dem nDSG verlangt. Wichtig dabei ist auf die Vollständigkeit und Verständlichkeit zu achten. Die Datenschutzerklärung muss als eigene Seite vorhanden sein, sie darf nicht in den AGBs versteckt werden. Weiter muss die Datenschutzerklärung leicht und einfach erreichbar sein.

Die gängige Praxis ist über den Footer am Ende jeder Webseite. Dabei ist zu beachten, dass sie nicht durch ein Cookie-Banner verdeckt werden darf. Dies gilt auch für Formulare, welche in den Vordergrund gerückt werden. Solange der Verweis auf die Datenschutzerklärung sichtbar bleibt, ist alles im grünen Bereich. Kritisch wird es bei Formularen, welche die ganze Seite füllen. Theoretisch müsste auch hier jeweils ein Link oder mindestens eine Information zur Datenschutzerklärung vorhanden sein.

Die Datenschutzerklärung muss nach nDSG nicht bestätigt werden. Es gilt lediglich die Pflicht der Information. Ein Opt-in ist daher überflüssig, es gibt aber auch keine Regelung dagegen.

2.6.1 Aktualität

Es gibt keine genaue Vorschrift, wie aktuell eine Datenschutzerklärung sein muss. Sie sollte jedoch alle sechs bis zwölf Monate überprüft werden. Gerade wenn ein Datum zur letzten Aktualisierung sichtbar ist, sollte man lieber alle sechs Monate drüber schauen.

2.7 Gibt es einen Datenschutzberater?

Nach nDSG gibt es die Rolle des Datenschutzberaters, in der DSGVO wird von einem Datenschutzbeauftragten gesprochen.
Das nDSG schreibt keine Pflicht für einen Datenschutzberater vor. Es gibt genau eine Situation, in welcher ein Vorteil entsteht, falls man trotzdem einen Datenschutzberater ernennt. Sollten Personendaten bearbeitet werden und es besteht ein hohes Risiko für die Person, muss eine Datenschutz-Folgenabschätzung durchgeführt werden. Wird nach deren Analyse trotz Massnahmen noch immer ein hohes Risiko erkannt, dann

kann dieses mit dem Datenschutzberater besprochen werden. Ist kein Datenschutzberater vorhanden, müssen die Ergebnisse an den Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) gemeldet werden.
Diese Situation stellt eine absolute Ausnahme dar und wird in der Praxis kaum auftreten.

Nach DSGVO ist ein Datenschutzbeauftragter Pflicht, wenn eine regelmässige und systematische Überwachung erfolgt oder besonders schützenswerte Personendaten bearbeitet werden.

Achtung!
Deutschland ist ein Ausnahmefall. Das Bundesdatenschutzgesetz (BDSG) schreibt einen Datenschutzbeauftragten als Pflicht vor, sobald sich mindestens 20 Personen im Unternehmen ständig mit der automatisierten Bearbeitung personenbezogener Daten beschäftigen. Dabei reicht der Versand von E-Mails bereits aus.

2.7.1 Kurzfassung

Nach nDSG gibt es keine Pflicht.
Nach DSGVO gibt es eine Pflicht in Ausnahmefällen.
Nach BSDG gibt es eine Pflicht, wenn mehr als 20 Mitarbeiter mit personenbezogenen Daten arbeiten.

Es ist jedoch auch ohne Pflicht sinnvoll zumindest intern eine Person zu bestimmen, welche sich vertieft mit dem Datenschutz und allenfalls nötigen Vorgängen auskennt. Gerade mit Blick auf die Auskunftspflicht oder Löschanträge, ist es sinnvoll festzulegen in wessen Aufgabenbereich dies fällt.

2.8 Ablaufplan für Anfragen

Durch das nDSG wird es möglich als Privatperson bei Unternehmen nachzufragen, welche Daten über einem gespeichert sind und diese zur Einsicht zu verlangen. Auch kann ein Antrag auf die Löschung aller vorhandenen personenbezogenen Daten gestellt werden. Welche Daten alles herausgegeben oder gelöscht werden müssen, kann aus dem Bearbeitungsverzeichnis herausgelesen werden.

Bei einem Löschantrag können Daten behalten werden, welche aktiv von hohem Interesse sind. Diese Ausnahme tritt beispielsweise in Kraft, wenn ein Löschantrag eingeht, die betroffene Person aber noch offene Rechnungen hat. Hier wäre eine Löschung aller Daten schlecht für das Geschäft. Nachdem alle offenen Rechnungen beglichen sind, müssen die verbliebenen Daten ebenfalls gelöscht werden.
Wichtig dabei ist, dass auch eine Anonymisierung der Daten als Löschung zählt. Die Daten dürfen am Ende keiner Person mehr zugeordnet werden können.

Ein Ablaufplan oder eine Vorbereitung ist weder nach nDSG noch DSGVO Pflicht. Es gilt jedoch eine Frist von 30 Tagen, um der Anfrage nachzukommen.

2.8.1 Wie wird die Identität des Antragstellers geprüft?

Jeder kann einen Antrag auf Datenherausgabe stellen, daher muss geprüft werden, ob die Person wirklich die ist, für die sie sich ausgibt. Die einfachste und praktischste Möglichkeit ist eine Kopie des Ausweises. Dies reicht als Absicherung nach nDSG aus.

2.9 Ablaufplan für Datenpannen vorhanden?

Genau wie der Ablaufplan bei einer Anfrage ist auch dieser Ablaufplan keine Pflicht, sondern reine Vorarbeit. Bei einer Datenpanne müssen nach nDSG die betroffenen Personen informiert werden so wie je nach Fall ein Bericht an den EDÖP erstellt werden. Die Informierung der Betroffenen kann beispielsweise per E-Mail oder Brief geschehen. Der EDÖP muss in der Regel nur benachrichtigt werden, wenn besonders schützenswerte Personendaten von der Datenpanne betroffen sind?

2.9.1 Was ist eine Datenpanne?

Nach nDSG kann man sich auf die Definition der «Verletzung der Datensicherheit» beziehen, welche folgenden definiert ist:
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.

Als Datenpanne gilt hier also sowohl ein Angriff als auch ein Unfall. Sollten versehentlich Daten gelöscht oder verändert werden, diese aber per Backup ohne weitere wieder hergestellt werden, so ist es in der Theorie zwar weiterhin eine Datenpanne, die Benachrichtigungspflicht dürfte in diesem Fall aber entfallen.

2.10 Sind die Mitarbeiter für den Datenschutz geschult?

Die grösste Datenschutzgefahr findet sich nicht in feindlichen Hackerangriffen, sondern in ungeschultem Personal. Wer mit Personendaten umgeht, muss die gängigen Gefahren kennen. Dazu zählt beispielsweise das Phishing. Mit gefälschten Mails, SMS oder Anrufen versuchen Betrügen, Sie auf eine betrügerische Webseite zu locken, Sie zur Eingabe von Daten in einem Online-Formular oder zum Öffnen eines mit Malware infizierten Dokuments in Ihrem Posteingang zu bewegen.

Gerade die neue Auskunftspflicht ist ebenfalls eine Möglichkeit an Daten zu gelangen, an welche ein Betrüger nicht gelangen sollte.

Ein weiterer Problempunkt sind Passwörter. Die beste Datenschutzerklärung hilft nicht, wenn am Ende Passwörter wie «Admin123» oder «MaxMuster1» genutzt werden. Hier empfiehlt sich eventuell auch ein Passwort Manager, welcher selbstständig Passwörter generiert und diese dann verwaltet.

2.11 Ist Google Analytics im Einsatz?

Google Analytics ist ein sehr mächtiges Tool. Im Grunde gibt es jedoch keine anderen Vorgaben als bei anderen Analysetools aus dem Ausland.
Zwingend wird die Kombination aus DPA-SCC-TIA benötigt. Sind alle diese drei Dokumente vorhanden, ist die wichtigste Absicherung passiert. Google Analytics muss weiter in der Datenschutzerklärung aufgelistet und erklärt werden.

2.11.1 Ist ein entsprechendes Consent Banner vorhanden? (Cookie Banner)

Ein Cookie Banner ist nach nDSG keine Pflicht. Eine Webseite, welche sich ausschliesslich an den schweizerischen Markt richtet, benötigt also kein Cookie Banner. Die reine Möglichkeit sich aus dem EU-Raum auf die Webseite zu begeben, reicht als Grundlage nicht aus. Erst wenn sich der Inhalt auch an EU-Bürger richtet, tritt die DSGVO mit einer Cookie Banner Pflicht in Kraft.
Bei einem Cookie Banner ist wichtig, dass nicht nur informiert wird, sondern auch die Möglichkeit gegeben ist, die Cookies abzulehnen.

2.11.2 Wann richtet sich eine Webseite an EU-Bürger?

Diese Frage ist schwerer zu beantworten. Ein Webshop, welcher ausschliesslich in die Schweiz liefert, ist beispielsweise für die EU relativ belanglos. Eine Webseite, welche die neusten Informationen zu Sportanlässen oder Festivals aufzeigt, kann für EU-Bürger dagegen durchaus relevant sein.
Um sicher zu sein, empfiehlt es sich, eine Möglichkeit zu finden, Zugriffe aus der EU zu filtern und diesen ein entsprechendes Banner anzuzeigen. In der Praxis wird auf die Filterung meistens verzichtet und die Banner werden allen Personen angezeigt.

2.12 Notfallplan bei „Abmahnung“ vorhanden?

Durch die DSGVO haben es sich einige Kanzleien zur Aufgabe gemacht, Abmahnungen auf Vorrat zu verschicken. Auch Privatpersonen drohen gerne damit, rechtliche Schritte zu starten. Gerade Google Analytics ist ein beliebtes Ziel, da leicht zu erkennen ist, ob es im Einsatz ist und Daten dabei an die USA weitergegeben werden.
Hier ist jetzt wichtig, dass die Konstruktion aus DPA-CSS-TIA vorhanden ist. Sind alle diese drei Teile gemacht worden, besteht wenig Grund zur Sorge. Die Dokumente können an die Kanzlei gesendet werden, welche dann in den meisten Fällen keine weiteren Schritte mehr unternimmt.

Auch wenn solche Anfragen und Androhungen mühsam sind und Zeit rauben, ist es wichtig höflich zu bleiben. Gerade private Datenschützer verbeissen sich sonst nur noch mehr darin, ob sie nicht doch einen Fehler im Datenschutz finden.

2.13 Werden Newsletter angeboten?

Newsletter gelten als Werbung, daher werden diese hauptsächlich durch das Bundesgesetz

gegen den unlauteren Wettbewerb (UWG) reguliert und stellen im nDSG nur einen Nebenschauplatz dar. Der wichtigste Teil des nDSG ist dabei die Informationspflicht.

2.13.1 Wird darüber korrekt informiert?

Über den Newsletter muss an zwei verschiedenen Stellen informiert werden. Einerseits in der Datenschutzerklärung, anderseits direkt bei der Newsletter Anmeldung selbst. Bei der Newsletter Anmeldung sollte der Inhalt und die Häufigkeit des Newsletters erwähnt sein. Beim Inhalt reicht eine thematische Angabe, es muss kein Musternewsletter abgebildet werden. Weiter sollte dabei eine Verlinkung zur Datenschutzerklärung vorhanden sein. Ist diese im Footer vorhanden und wird nicht überdeckt, reicht die Information ohne Verlinkung aus.

Wird der Newsletter per Checkbox angeboten, so darf diese nach nDSG standardmässig aktiviert sein. Nach DSGVO darf die Option nicht bereits ausgewählt sein, sondern muss bewusst angeklickt werden.

2.13.2 Ist Double Opt-in Pflicht?

Weder nach nDSG noch DSGVO ist Double Opt-in eine direkte Pflicht. Sollte jedoch ein Rechtsstreit ausbrechen, wird ein Nachweis der bewussten Einwilligung des Empfängers verlangt. Dieser Nachweis ist nur durch ein Double Opt-in sichergestellt. Das bedeutet, ohne Double Opt-in entsteht kein Problem durch das nDSG oder die

DSGVO, sondern durch das UWG (sowohl in der Schweiz als auch der EU).
Es ist daher klar empfehlenswert Double Opt-in zu nutzen.

2.13.3 Ist ein Opt-out vorhanden?

Von einem Newsletter sollte man sich einfach und ohne Mühe abmelden können. Die gängige Praxis dazu ist ein Abmeldungslink im Footer des Newsletters. Dabei muss die Abmeldung direkt erfolgen, es dürfen keine Daten oder Gründe verlangt werden. Man kann jedoch die Option anbieten auf freiwilliger Basis mitzuteilen, warum der Newsletter abbestellt wurde.

Achtung!
Auch wenn ein solcher Link zu Abmeldung vorhanden ist, müssen auch Abmeldungen auf andere Art umgesetzt werden. Ruft eine Person an oder meldet sich per Brief, so zählt auch dies als legaler Weg zur Abmeldung.

2.14 Gibt es anderen E-Mail-Versand?

Gerade im E-Commerce Bereich werden weitere E-Mails versendet. Dies geht von Bestellbestätigungen bis zu Erinnerung zur Produktbewertung. Für solche E-Mails stellt sich eine zentrale Frage.

2.14.1 Handelt es sich dabei um Werbung?

Reine Informationsnachrichten können ohne weitere Zustimmung versendet werden. Dazu zählen Änderungen an den AGBs, Bestellbestätigungen, Rechnungen oder rein informative Neuigkeiten des Unternehmens (Übernahme, Schliessung, etc.).

Kritisch wird es, wenn eine solche Nachricht mit Werbung verbunden wird. Beispielsweise zählt eine Bestellbestätigung mit weiteren Produkten im Footer als Werbung. Theoretisch wäre dazu ebenfalls eine Bestätigung erforderlich.

Reine Werbenachrichten benötigen genau wie ein Newsletter eine Zustimmung per Double Opt-in mit einfachem Opt-out.

2.14.2 Ausnahme der Schweiz

Die Schweiz hat eine Ausnahme bei Werbung, welche dem E-Commerce zugutekommt. Werden die Kontaktinformationen beim Kauf hinterlegt und ist ein Hinweis auf ein einfaches Opt-out vorhanden, dann dürfen weitere E-Mails mit

ähnlichen Waren versendet werden. Dazu zählen auch Erinnerungen zu Produktbewertungen oder befüllten Warenkörben.

Der sicherste Weg, um sowohl in der Schweiz als auch der EU jedes Risiko zu minimieren, bleibt jedoch ein Double Opt-in zu jeder Kategorie von E-Mails, welche nicht rein informativ sind.

2.15 Werden Mails per Drittanbieter versendet?

Wird ein Drittanbieten genutzt, so tritt das nDSG bezüglich der Datenbearbeitung in Kraft. Auch der Versand rein informativer E-Mails ohne Werbezweck wird als Datenbearbeitung gewertet und benötigt die entsprechenden Schritte.
Siehe dazu die Punkte 3 – 5.

2.16 Gibt es Verlinkungen auf Drittseiten?

Grundsätzlich ist eine reine Verlinkung auf eine Drittseite kein Problem, da dabei keine Daten übertragen werden. Wichtig dabei ist jedoch, dass auch bei entsprechendem Vermerk im Datenschutz, dass man jegliche Haftung ablehne für deren Inhalt, man trotzdem teilweise haftbar gemacht werden kann. Es ist daher sinnvoll in einem angemessenen Rahmen Verlinkungen auf Drittseiten zu prüfen, ob noch das gewünschte Ziel erreicht wird.

2.16.1 Handelt es sich dabei um Social Media?

Social Media fällt je nach Verlinkung und Einstellung in eine Sonderkategorie. Handelt es sich lediglich um eine Weiterleitung, fallen keine extra Regelungen an. Das Problem ist jedoch, dass Social Media Integrationen gerne schon vor einem aktiven Anklicken des Links Daten sammeln. Dabei reicht die IP-Adresse damit es sich um personenbezogene Daten handelt. Wenn dies passiert, ist nach nDSG ein Datenbearbeitungsvertrag Pflicht.

Ebenfalls wichtig ist es, die entsprechenden Social Media in der Datenschutzerklärung zu erwähnen und falls Daten geschickt werden, auszulisten um welche Daten es sich handelt.

3. Vorlagen / Muster

Die Muster sind von verschiedenen Onlineanbietern übernommen. Es gibt keine Garantie auf Vollständigkeit. Keines dieser Muster ist als feste Vorgabe zu verstehen, es soll lediglich als Beispiel einer möglichen Umsetzung dienen. Die eigene Umsetzung darf (und soll meistens auch) davon abweichen.

3.1 Beispiel für Dateninventar/Bearbeitungsverzeichnis

Da das Dateninventar als Grundlage für das Bearbeitungsverzeichnis dient, werden hier beide zusammengefasst.

Muster:
https://www.lda.bayern.de/media/muster/muster_9_online-shop_verzeichnis.pdf

https://www.lda.bayern.de/media/dsk_muster_vov_verantwortlicher.pdf

Checkliste für den Inhalt:

	nDSG	DSGVO
Verantwortlicher	✅	✅
Datenschutzbeauftragter		✅
Bearbeitungszwecke	✅	✅
Betroffene Personen (Kategorien)	✅	✅
Bearbeitete Personendaten (Kategorien)	✅	✅
Empfängerinnen (Kategorien)	✅	✅
Aufbewahrungsdauer (oder Kriterien für Festlegung)	✅	✅
Daten-Export (Staaten, evtl. Garantien)	✅	✅
TOM	✅	✅

3.2 Beispiel für Auftragsbearbeitungsvertrag

Viele internationale Unternehmen haben durch die DSGVO oder andere Datenschutzgesetze bereits einen DPA. In den meisten Fällen kann dieser mit wenig Aufwand abgeschlossen werden.

Vorlage nach DSGVO:
https://www.5001.ch/wp-content/uploads/2022/06/Muster_Auftragsverarbeitungsvertrag-3509265-3509310.pdf

Beispiel:
Zoom: https://explore.zoom.us/docs/doc/Zoom_GLOBAL_DPA.pdf
Mailchimp: https://mailchimp.com/de/legal/data-processing-addendum/

3.3 Beispiel Standarddatenschutzklausel

Für die Umsetzung der SCC kann die Vorlage der EU genutzt werden. Diese wird für das nDSG aktzeptiert.

Vorlage der EU:
https://commission.europa.eu/documents_en (nach «Standard contractual clauses for controllers and processors in the EU/EEA» suchen)

Generator:
https://shop.haerting.ch/scc-generator/ (Achtung kostenpflichtig)

3.4 Transfer Impact Assessment

Die bekannteste Methode in der Schweiz wurde von David Rosenthal entwickelt und kann auf seiner Webseite kostenlos heruntergeladen werden.

Muster:
https://www.rosenthal.ch/ (Hauptseite)
https://www.rosenthal.ch/downloads/Rosenthal_EU-SCC-TIA.xlsx (Direktdownload)

3.5 Datenschutzerklärung

Die Datenschutzerklärung gehört zu den Standarddokumenten. Eine Datenschutzerklärung ist Pflicht, sowohl nach Schweizer Recht als auch nach DSGVO.

Vorlage:
https://dsat.ch/download/3/dsat/411/dsat-ch-vorlage-datenschutzerklaerung-v2-01-2.pdf

Generator:
https://www.datenschutzpartner.ch/angebot-datenschutz-generator/ (Achtung kostenpflichtig)

3.6 Cookie Banner

Beim Cookie Banner ist es wichtig zu verstehen, dass es kein Zwang sein darf, alle Cookies zu akzeptieren. Es muss die Möglichkeit geben, die Cookies abzulehnen.

Cookie Banner Generator:
https://www.freeprivacypolicy.com/free-cookie-consent/

Cookie Banner Modul:
https://amasty.com/cookie-consent-for-magento-2.html

3.7 Newsletter

Kurzfassung zu Inhalt und Häufigkeit:

«Der Newsletter informiert über unsere neusten Produkte sowie Sonderaktionen. Er wird jeweils zu Beginn des Monats versendet. Weitere Informationen finden Sie in unserer Datenschutzerklärung.»

4. Quellen

https://www.datenschutzpartner.ch/n-dsg/

https://static1.squarespace.com/static/606433e92bb6af0775657d3c/t/638890170b94ba73474a2bf7/1669894167520/221201_Datenschutz_DINA4_wickipartners.pdf

https://www.datenschutzpartner.ch/2023/02/16/webinar-auftragsverarbeitungsvertrag-20230216/

https://www.datenschutzpartner.ch/2021/10/26/webinar-verzeichnis-bearbeitungstaetigkeiten_20211026/

https://www.datenschutzpartner.ch/2022/09/06/webinar-countdown-neues-datenschutzgesetz-20220906/

https://www.datenschutzpartner.ch/2023/05/02/legal-session-fragen-datenschutzrecht-20230502/

https://www.datenschutzpartner.ch/2023/03/07/legal-session-fragen-datenschutzrecht-20230307/

https://www.datenschutzpartner.ch/2023/05/30/legal-session-fragen-datenschutzrecht-20230530/

https://www.datenschutzpartner.ch/2022/10/04/webinar-newsletter-20221004/

https://www.fedlex.admin.ch/eli/cc/1988/223_223_223/de

https://www.datenschutzpartner.ch/2022/06/21/legal-session-fragen-datenschutzrecht-20220621/