MME

Checkliste neues Datenschutzrecht in der Schweiz

Das neue schweizerische Datenschutzgesetz (nDSG) und seine zugehörige Verordnung über den Datenschutz (DSV) treten am 1. September 2023 in Kraft.

Diese Checkliste soll der Umsetzung der Anforderungen aus dem nDSG und der DSV für private Unternehmen dienen (und nicht Bundesorganen oder in deren Auftrag handelnden privaten Unternehmen).

Die Checkliste ist nicht abschliessend. Weitere Anforderungen an die «Compliance» können sich aus anderweitigen rechtlichen Bestimmungen, insbesondere sektorspezifischen Regelungen oder Branchenanforderungen und insbesondere aus der Datenschutz-Grundverordnung der EU (DSGVO) ergeben. Die DSGVO kann aufgrund ihrer exterritorialen Wirkung auch für Schweizer Unternehmen Anwendung finden, wenn die Datenverarbeitung im Zusammenhang damit steht, betroffenen Personen in der Europäischen Union (EU)/ im EWR Waren oder Dienstleistungen anzubieten oder das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der EU/ im EWR erfolgt (Art. 3 DSGVO). Die entsprechenden Bestimmungen sind daher allenfalls zusätzlich zu beachten.

Die vorliegende Checkliste erhebt keinen Anspruch auf Vollständigkeit und stellt keine Rechtsberatung dar.

Aufgabe/Dokument	Anmerkung	Zwingend?	Rechtliche Vorschrift	Erfolgt?
Datenschutzkonzept	Regelt die Verantwortlichkeiten im Unternehmen für eine rechtlich konforme Datenbearbeitung und legt das Niveau des Datenschutzes fest („Setting the tone at the top“).	Faktisch ja, insbesondere im Hinblick auf mögliche Haftungsrisiken.	n/a	☐
Review Arbeitsverträge	- Ausdrückliche Geheimhaltungsvereinbarung - Verweise auf Datenschutzerklärung für Mitarbeitende (nicht zum Vertragsbestandteil machen!)	Nein, aber faktisch zwingend um in der EU in den Genuss der schützenden Bestimmungen der Richtlinie (EU) 2016/943 über den Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung (bzw. der entsprechenden nationalen Gesetze zu deren Umsetzung) zu gelangen. Denn anders als im Schweizer Recht müssen Unternehmen danach aktiv werden und „angemessene Geheimhaltungsmassnahmen“ ergreifen, damit entsprechender Schutz erreicht wird. Dazu kann im Rahmen eines Geheimnisschutzkonzepts auch die Vereinbarung von Verschwiegenheitsklauseln dienen. Zudem, bei Bestehen von Berufsgeheimnispflichten sinnvoll.	n/a	☐
Datenschutzerklärung „nach Aussen“ = Datenschutzerklärung für Kunden und Geschäftspartner etc.	Allgemeine Datenschutzerklärung auf der Webseite über den Umgang mit Personendaten von Kunden, Geschäftspartner etc, einschliesslich Cookies.	Ja	Art. 19-21 nDSG	☐

Aufgabe/Dokument	Anmerkung	Zwingend?	Rechtliche Vorschrift	Erfolgt?
Datenschutzerklärung „nach Innen“ = Datenschutzerklärung für Mitarbeiter und Bewerber	Information an Mitarbeitende und Bewerber über die Bearbeitung ihrer Personendaten, insbesondere auch über Austausch von Daten innerhalb des Konzerns. Üblicherweise in zwei separaten Dokumenten, in einem für Mitarbeitende und einem für Bewerber.	Ja	Art. 19- 21 nDSG	☐
Datenschutzrichtlinie für Mitarbeitende bzgl. deren Umgang mit Personendaten	Allgemeine Leitlinien und Weisungen zum Umgang mit Personendaten, einschliesslich Verwendung neuer IT-Tools.	Nicht direkt, aber der Verantwortliche ist verpflichtet, die Datenbearbeitung technisch und organisatorisch so auszugestalten, dass die Datenschutzvorschriften eingehalten werden.	vgl. Art. 6-8 nDSG	☐
Richtlinie zur Nutzung von IT/Telefon/Home Office	Richtlinien zum Umgang mit IT/Telefon/Home Office sowie allenfalls Information über die Auswertung bestimmter Verhaltensdaten.	Ja, falls die erforderlichen Informationen zur Auswertung bestimmter Verhaltensdaten nicht schon in der Datenschutzerklärung „nach Innen“ enthalten sind. Im Übrigen nicht direkt zwingend, aber notwendig, z.B. um gewisse Weisungen zu erteilen (bspw. bzgl. privater Nutzung der IT/Telefonie).	vgl. Art. 6-8 nDSG, zudem Art. 19-21 nDSG	☐
Schulungen	Regelmässige Schulungen über den Umgang mit Personendaten für Mitarbeitende.	Nein, aber sinnvoll aus den gleichen Erwägungen wie bei „Datenschutzrichtlinie für Mitarbeitende“.	n/a	☐
Prüfung/Abschluss weiterer Verträge	Auftragsdatenbearbeitungsverträge, Joint-Controller, Controller-to-Controller, AGBs.	Ja, Auftragsbearbeitungsverträge sind zwingend. Die übrigen Verträge sind nach Schweizer Recht nicht zwingend, aber in der Regel sinnvoll.	Art. 9 nDSG	☐

Aufgabe/Dokument	Anmerkung	Zwingend?	Rechtliche Vorschrift	Erfolgt?
		Zudem empfehlen wir Verweise auf die Datenschutzerklärung in AGBs und sonstiger geschäftlicher Korrespondenz (Offerten, Rechnungen etc.).		
Intra-Company Agreement für den Datenaustausch innerhalb des Konzerns	Interne vertragliche Vereinbarung von Unternehmen des gleichen Konzerns, welche den Austausch von Daten und die jeweiligen Rollen/Verantwortlichkeiten innerhalb des Konzerns regelt.	Ja, zwingend in Bezug auf Auftragsbearbeitungsverhältnisse. Im Übrigen unbedingt zu empfehlen.	Art. 9 nDSG	☐
Datenschutz-Folgenabschätzung (DSFA) bei möglicherweise hohem Risiko (z.B. allenfalls bei AI Tools, Zutrittskontrollen unter Verwendung von biometrischen Systemen, Verwendung von Tracking-Tools)	Risikoeinschätzung bzgl. der Datenbearbeitung. Die DSFA ist nach Beendigung der Datenbearbeitung für mindestens zwei Jahre aufzubewahren.	Ja, wenn sich aus der Datenbearbeitung ein hohes Risiko für die Persönlichkeit oder Grundrechte der betroffenen Person ergeben kann, insbesondere bei umfangreicher Bearbeitung besonders schützenswerter Daten oder bei Profiling mit hohem Risiko.	Art. 22-23 nDSG, Art. 14 DSV	☒
Datentransfer ins Ausland	Wenn Daten in ein Land ohne angemessenen Datenschutz übermittelt werden, muss ein angemessenes Datenschutzniveau auf andere Weise hergestellt werden (z.B. über die Standardvertragsklauseln der EU «SCCs», welche auf das Schweizer Recht angepasst werden müssen «Swiss Finish»).	Ja, es sei denn, es besteht eine Ausnahme. Bei der Verwendung vertraglicher Garantien muss zudem ein so genanntes «Transfer Impact Assessment» durchgeführt werden, um sich eines angemessenen Datenschutzes zu vergewissern.	Art. 16, 17 nDSG, Art. 9ff. DSV	☐
Umgang mit Betroffenenrechten	Recht auf Auskunft, Berichtigung, Löschung, Widerspruch, Datenportabilität.	Prozesse und Muster-Korrespondenz für den Umgang mit Betroffenenrechten sind rechtlich nicht zwingend, müssen	Art. 25-29 nDSG, Art. 41	☐

Aufgabe/Dokument	Anmerkung	Zwingend?	Rechtliche Vorschrift	Erfolgt?
		aber faktisch funktionieren. Beispielsweise müssen Auskunftsersuchen in der Regel innerhalb von 30 Tagen beantwortet werden. Bei grösseren Unternehmen und häufigen Betroffenenbegehren faktisch zwingend. In allen anderen Fällen kann auch eine kurze interne Richtlinie und die Behandlung der Begehren im Einzelfall ausreichen.	nDSG, Art. 16-22 DSV	
Besondere Anforderungen: Datenportabilität	Betroffene Personen können vom Verantwortlichen die Herausgabe bestimmter Personendaten in einem gängigen elektronischen Format verlangen, wenn der Verantwortliche die Daten automatisiert bearbeitet und die Daten mit Einwilligung der betroffenen Person oder in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags mit dem Verantwortlichen und der betroffenen Person bearbeitet werden.	Ja, wenn keine Ausnahme besteht. Erfordert entsprechende technische Umsetzung und fristgerechte Erfüllung etwaiger Anfragen.	Art. 28-29 nDSG, Art. 20-22 DSV	☐
Besondere Anforderungen: Automatisierte Einzelentscheidungen	Entscheidungen, die ausschliesslich auf einer automatisierten Bearbeitung beruhen und die für die betroffene Person mit einer Rechtsfolge verbunden sind oder sie erheblich beeinträchtigen (z.B. automatische Ablehnung eines Kredits, automatische Ablehnung von Bewerbern). In diesen Fällen muss der Verantwortliche die betroffene Person über die automatisierte Einzelentscheidung im	Ja.	Art. 21 nDSG	☐

Aufgabe/Dokument	Anmerkung	Zwingend?	Rechtliche Vorschrift	Erfolgt?
	Rahmen der Datenschutzerklärung oder individuell informieren und ihr auf Antrag die Möglichkeit geben, ihren Standpunkt darzulegen. Zudem kann die betroffene Person verlangen, dass die automatisierte Einzelentscheidung von einer natürlichen Person überprüft wird.			
Datensicherheit	Verantwortliche und Auftragsbearbeiter müssen durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit gewährleisten mit dem Ziel der Sicherstellung der Vertraulichkeit, Verfügbarkeit und Wiederherstellbarkeit der Daten, ihrer Integrität und Nachvollziehbarkeit.	Ja.	Art. 8 nDSG, Art. 1 ff. DSV	☐
Berechtigungskonzept bzgl. Zugriff auf Personendaten	Teil der Massnahmen zur Datensicherheit.	Faktisch ja, siehe Ausführungen zur „Datensicherheit“.	Art. 8 nDSG, Art. 3 Abs. 1 DSV	☐
Protokollierung	Wenn besonders schützenswerte Personendaten in grossem Umfang automatisierte bearbeitet werden oder ein Profiling mit hohem Risiko durchgeführt wird und die präventiven Massnahmen den Datenschutz nicht gewährleisten, so müssen der Verantwortliche und der Auftragsbearbeiter zumindest das Speichern, Verändern, Lesen, Bekanntgeben, Löschen und Vernichten von Personendaten protokollieren. Die Protokolle müssen mindestens während einem Jahr getrennt vom	Ja, unter den genannten Voraussetzungen.	Art. 8 nDSG, Art. 4 DSV	☐

Aufgabe/Dokument	Anmerkung	Zwingend?	Rechtliche Vorschrift	Erfolgt?
	System, in welchem die Personendaten bearbeitet werden, aufbewahrt werden.			
Meldung und Dokumentation von Verletzungen der Datensicherheit	Verletzungen der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führen, müssen dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) so rasch als möglich gemeldet werden. Darüber hinaus sind die betroffenen Personen zu informieren, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB dies verlangt. Verletzungen der Datensicherheit müssen dokumentiert werden. Die Dokumentation ist für mindestens zwei Jahre aufzubewahren.	Ja, unter den genannten Voraussetzungen.	Art. 24 nDSG, Art. 15 DSV	☐
Datenlöschkonzept (Data Retention Policy) und entsprechende Umsetzung	Personendaten müssen vernichtet oder anonymisiert werden, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind und keine Aufbewahrungspflichten oder sonstige Rechtfertigungsgründe mehr bestehen.	Ja.	Art. 6 Abs. 4 nDSG	☐
Bearbeitungsverzeichnis für den Bereich HR (und für alle anderen Bereiche) Ausnahme für Unternehmen mit < 250 Mitarbeitenden sofern deren Datenbearbeitungen nur ein geringes Risiko mit sich bringt	Verantwortliche und Auftragsbearbeiter müssen ein Verzeichnis ihrer Bearbeitungstätigkeiten führen. Dieses enthält bestimmte Mindestangaben (z.B. die Kategorien bearbeiteter Personendaten, Kategorien der betroffenen Personen, den Bearbeitungszweck etc.) und muss auf aktuellem Stand gehalten werden.	Ja, es sei denn es besteht die genannte Ausnahme. In der Praxis aber eigentlich immer zu empfehlen, um einen strukturierten Überblick über die Datenbearbeitungen zu erhalten.	Art. 12 nDSG, Art. 24 DSV	☐

Aufgabe/Dokument	Anmerkung	Zwingend?	Rechtliche Vorschrift	Erfolgt?
Bearbeitungsreglement	Das Bearbeitungsreglement muss Angaben zur internen Organisation, zu Datenbearbeitungs- und Kontrollverfahren sowie zu den Massnahmen zur Gewährleistung der Datensicherheit enthalten.	Ja, wenn besonders schützenswerte Personendaten in grossem Umfang bearbeitet werden oder ein Profiling mit hohem Risiko durchgeführt wird.	Art. 5-6 DSV	☐
Bestellung eines (externen oder internen) Datenschutzberaters	Anlaufstelle für betroffene Personen und für den EDÖB. Aufgaben: Beratung und Mitwirkung bei der Anwendung der Datenschutzvorschriften.	Nein, nach Schweizer Recht optional.	Art. 10 nDSG	☐
Datenschutzkoordinator	Interne Anlaufstelle. Aufgabe: Koordination der Datenschutzthemen.	Nicht direkt, aber faktisch zwingend (Teil des Datenschutzkonzepts, siehe Ausführungen zum „Datenschutzkonzept“).	n/a	☐
Vertreter in der Schweiz	Unter bestimmten Voraussetzungen müssen ausländische Unternehmen einen Vertreter in der Schweiz benennen.	Ja.	Art. 14-15 nDSG	☐

Stand: 31.08.2023

Ihr Kontakt für Rückfragen zum Thema Datenschutzrecht:

MME Legal, Caroline Gaul, Legal Partner, +41 44 254 99 66, caroline.gaul@mme.ch