walderwyss

Walder Wyss AG
Seefeldstrasse 123
Postfach
8034 Zürich
Schweiz
Telefon +41 58 658 58 58
Telefax +41 58 658 59 59
www.walderwyss.com

Revidiertes Datenschutzrecht der Schweiz: Umsetzung durch KMU

Stand: 9. März 2023

David Vasella
Partner
Dr. iur., CIPP/E, CIPM, FIP
Rechtsanwalt
direkt +41 58 658 52 87
david.vasella@walderwyss.com

1. Weisungen und Dokumentation
2. Datenschutz-Organisation
3. Bearbeitungsverzeichnis und Bearbeitungsreglement
4. Information und Datenschutzerklärungen
5. Betroffenenrechte
6. Vertragsbestimmungen
7. Übermittlung ins Ausland
8. Compliance- und Risikoprüfungen
9. Daten von Mitarbeitenden
10. Datensicherheit
11. Datenlöschung

Dieses Dokument enthält eine Checkliste für die Umsetzung des revidierten schweizerischen Datenschutzgesetzes (**nDSG**) und der zugehörigen revidierten Datenschutzverordnung (**DSV**). Beide treten am 1. September 2023 in Kraft. Übergangsfristen gelten nur für bestimmte Anforderungen.

Die Checkliste ist auf einfachere Verhältnisse und private Unternehmen ausgelegt (nicht für öffentliche Organe). Grössere Organisationen werden diverse interne Vorgaben und Prozesse definieren müssen, um die Anforderungen einhalten zu können, auch wenn das nDSG und die DSV solche Prozesse kaum ausdrücklich verlangen.

Rot sind zwingende Aufgaben hinterlegt, gelb Aufgaben, die als möglicherweise zwingend zu prüfen oder die faktisch notwending sind, und grün Aufgaben, die sinnvoll, aber optional sind.

Diese Checkliste berücksichtigt ausschliesslich das nDSG und die DSV und am Rande Geheimnisschutzbestimmungen, aber weder weitere Anforderungen aus sektoriellen Regelungen noch die Europäische Datenschutz-Grundverordnung (**DSGVO**). Letztere ist vor allem dann – zusätzlich zum nDSG – einzuhalten, wenn ein schweizerisches Unternehmen eine Niederlassung im EWR-Ausland hat, Angebote gezielt auf natürliche Personen im EWR ausrichtet oder das Verhalten von Personen im EWR-Ausland beobachtet (z.B. durch ein Tracking), und dann, wenn interne oder externe Vorgaben die Einhaltung der DSGVO verlangen.

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

1. Weisungen und weitere Dokumentation

Anders als die DSGVO kennt das schweizerische Datenschutzrecht keine allgemeine Dokumentationspflicht und entsprechend keine Pflicht, Richtlinien zu erlassen. Es ist aber faktisch zwingend, zumindest die wesentlichsten Grundsätze in Form einer Weisung oder einer Handlungsanleitung festzulegen.

Minimalaufgaben:

— Abläufe und Organisation durchdenken

— wesentlichen Vorgaben und Aufgaben als Richtlinie oder zumindest Twopager aufschreiben

Dokument/Aufgabe	*Anmerkungen*	*Zwingend?*	*Grundlage*
Richtlinie zum Datenschutz	Dokument mit allgemeinen Leitlinien und Weisungen für den Umgang mit Personendaten	Nein, aber sinnvoll aus Grundlage der korrekten internen Delegation von Aufgaben, als arbeitsrechtliche Weisung, als Grundlage weiterer Weisungen und zur Schulung.	n/a
Weitere Richtlinien	Dokumente mit weiteren Vorgaben bspw. zum Umgang mit IT-Mitteln und zur Auswertung bestimmter Verhaltensdaten durch den Arbeitgeber.	Nicht direkt, aber sinnvoll, aber jedenfalls die Auswertung bspw. des E-Mail-Verkehrs und weiterer Verhaltensdaten verlangt zumindest laut dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) entsprechende vorgängige Hinweise.	Art. 6 und 19 nDSG; Art. 321b OR
«Twopager» zum Datenschutz	Knappes Dokument zuhanden der Mitarbeitenden mit praktischen Hinweisen zum Umgang mit Datenschutzthemen, z.B. bei neuen Tools auf der Website und sonstigen neuen oder geänderten Bearbeitungen, Betroffenenbegehren, Datenschutzverletzungen usw., und zur Geheimhaltung von Personendaten	Nicht direkt, aber faktisch zwingend, wenn nicht andere Richtlinien und Prozesse existieren. Es kann in grösseren Unternehmen zudem als Übersicht und «Field Guide» dienen.	n/a

«Logbuch» zum Datenschutz	Ein Dokument oder eine Intranetseite, auf der Datenschutzvorfälle erfasst werden können (bspw. Betroffenenbegehren, Sicherheitsverletzungen oder durchgeführte Datenschutz-Folgenabschätzungen)	Nein, das nDSG verlangt keine systematische Aufzeichnung solcher Vorgänge. Es kann aber intern hilfreich sein und bei Bedarf auch gegen aussen, bspw. im Fall des Verkaufs eines Unternehmens	n/a
Schulungsunterlagen	Eine Datenschutzschulung ist sinnvoll, besonders für Mitarbeitende, die im Rahmen der Datenschutzcompliance bestimmte Aufgaben haben (z.B. im Bereich HR, IT, Legal usw.).	Nein, zwingend ist eine Datenschutzschulung nicht, aber sie wird normalerweise erforderlich sein, in einer der Organisation angepassten Weise.	n/a

2. Datenschutz-Organisation

Das nDSG kennt nur wenige ausdrückliche Anforderungen an die Organisation im Bereich des Datenschutzes. Faktisch werden allerdings bei den meisten Unternehmen bestimmte organisatorische Vorkehrungen zu treffen sein.

Minimalaufgaben:

— Bedarf, vorhandene Ressourcen, Abläufe und Zuständigkeiten durchdenken

— ggf. entsprechende Funktionen bestimmen und i.d.R. in einer Richtlinie oder Weisung festhalten

Dokument/Aufgabe	*Anmerkungen*	*Zwingend?*	*Grundlage*
Bestellung eines Datenschutz-Beraters (DSB)	Ein DSB ist dafür zuständig, im Unternehmen pro- und reaktiv auf die Einhaltung des Datenschutzes hinzuweisen und als Anlaufstelle intern, für Betroffene und für den EDÖB zu fungieren.	Nein, die Bestellung eines DSB ist nach dem nDSG nicht zwingend, auch nicht bei heiklen Bearbeitungen. Es wird aber als Teil der Compliance empfunden und u.U. von Geschäftspartnern erwartet.	Art. 10 nDSG; Art. 23 und 25 f. DSV
Bestellung weiterer Datenschutz-Funktionen	Die Einhaltung des Datenschutzes kann nicht allein mit externen Ressourcen bewältigt werden – bestimmte interne Anlaufstellen sind fast immer unumgänglich, und seien es nur dedizierte Ansprechpersonen. Zudem sollte die Geschäftsleitung bzw. der VR das Thema ausreichend verstehen und vor allem auch ernst nehmen.	Nicht direkt, aber wenn der VR bzw. die GL das Thema ignorieren, haben sie u.U. Haftungsrisiken. Es sollte daher eine interne Stelle mit dem Thema betraut werden. Bei grösseren Unternehmen sollten in den produktiven Einheiten und Supportfunktionen Ansprechpersonen bestimmt werden.	n/a
Vertreter in der Schweiz	Das nDSG verlangt in Ausnahmefällen, dass ausländische Unternehmen in der Schweiz einen Vertreter bestellen.	Ja, wenn ausnahmsweise die entsprechenden Voraussetzungen erfüllt sind.	Art. 14 f. nDSG

3. Bearbeitungsverzeichnis und Bearbeitungsreglement

Unternehmen sind verpflichtet, ein Verzeichnis ihrer Bearbeitungstätigkeiten zu führen, das «Bearbeitungsverzeichnis», mit Ausnahme von KMU, die von dieser Pflicht unter Umständen befreit sind.

Minimalaufgaben:

— Vorlage eines Bearbeitungsverzeichnisses verwenden und befüllen und regelmässig à jour bringen (ausser es gilt die KMU-Ausnahme)

— prüfen, ob die Voraussetzungen eines Bearbeitungsreglements erfüllt sind; ggf. Bearbeitungsreglement erstellen (lassen)

Dokument/Aufgabe	*Anmerkungen*	*Zwingend?*	*Grundlage*
Bearbeitungsverzeichnis	Ein Verzeichnis der Art und Weise der Datenbearbeitungen mit bestimmten Mindestangaben (bspw. in Form eines Excel-Dokuments oder über die Plattform von Walder Wyss*).	Ja, wobei eine Ausnahme gilt für KMU mit weniger als 250 Mitarbeitenden per 1. Januar, soweit keine «besonders schützenswerten Personendaten» in grossem Umfang bearbeitet werden und kein «Profiling mit hohem Risiko» erfolgt.	Art. 12 nDSG; Art. 23 DSV
Prozess zur Nachführung des Bearbeitungsverzeichnisses	Es ist sinnvoll, einen Prozess für die Nachführung des Bearbeitungsverzeichnisses zu definieren, bspw. in Form einer Anweisung an das Business, im Fall neuer oder geänderter Bearbeitungen ein Update zu prüfen und ggf. einer Datenschutzfachstelle mitzuteilen.	Nein, ein solcher Prozess ist nicht zwingend. Das Bearbeitungsverzeichnis muss aber grundsätzlich auf dem aktuellen Stand gehalten werden. Bei nicht sehr übersichtlichen Verhältnissen ist zumindest ein rudimentärer Prozess erforderlich.	Art. 12 Abs. 1 nDSG
Bearbeitungsreglement	Eine Art Handbuch für den Datenschutz, das für eine oder mehrere Datenbearbeitungen gilt und die Organisation des Datenschutzes, die Funktionsweise	Ja, allerdings nur für automatisierte Bearbeitungen von besonders schützenswerten Personendaten in grossem Umfang und für ein Profiling mit hohem Risiko.	Art. 5 f. DSV

* Wir stellen eine Plattform für Datenschutzprojekte einschliesslich eines Tools für Bearbeitungsverzeichnisse zur Verfügung.

	der Systeme, die Schritte der Bearbeitung und die Datensicherheitsmassnahmen beschreibt. Das Reglement kann auf bestehende Dokumente verweisen und muss nicht detailliert sein.		

4. Information und Datenschutzerklärungen

Nach dem nDSG müssen Verantwortliche grundsätzlich über alle Beschaffungen von Personendaten informieren und dabei bestimmte Mindestangaben machen. Das gilt anders als nach heutigem Recht nicht nur für heikle Daten oder überraschende Bearbeitungen. Eine (eventual-)vorsätzliche Verletzung der Informationspflicht kann strafbar sein.

Minimalaufgaben:

— Ausarbeitung und Aufschalten einer allgemeinen Datenschutzerklärung (DSE)

— Ausarbeitung und Abgabe einer Datenschutzerklärung für Mitarbeitende

— Prüfung der Verträge bzw. AGB und sonstiger Dokumentation, ggf. Hinweise auf die DSE ergänzen und veraltete Datenschutzhinweise entfernen (siehe auch Ziff. 6 – Vertragsbestimmungen)

Dokument/Aufgabe	*Anmerkungen*	*Zwingend?*	*Grundlage*
Datenschutzerklärung – Allgemein	Eine allgemeine Datenschutzerklärung (DSE) auf der Website des Unternehmens, die Bearbeitungen von (End-)Kundendaten, Daten von Kontaktpersonen von Lieferanten und B2B-Kunden und weiteren Personen erläutert, besonders auch die Datenbeschaffung aus Drittquellen.	Ja, eine DSE ist zwingend, und eine allgemeine Datenschutzerklärung auf der Website ist oft eine faktisch zwingende Umsetzungsmassnahme.	Art. 19 f. und Art. 61 nDSG; Art. 13 DSV
Datenschutzerklärung – Online	Eine DSE, die den Umgang mit Cookies und weiteren Technologien, aber auch anderen Bearbeitung im Online-Bereich erläutert (in Apps, in einem Kontaktformular, durch elektronische Newsletter usw.).	Ja, eine solche DSE ist zwingend, sofern im Online-Bereich Personendaten bearbeitet werden. Sie entspricht heute auch in der Schweiz den Erwartungen des Publikums.	Art. 45c des Fernmeldegesetzes
Hinweise auf Datenschutzerklärungen	Auf Datenschutzerklärungen sollte an geeigneter Stelle hingewiesen werden (bspw. in AGB, bei Online-Formularen und Shops, in Rechnungen, auf Korrespondenz usw.).	Die genauen Anforderungen an Hinweise auf die DSE sind noch nicht klar, aber wo möglich, sollten die Betroffenen an den jeweiligen Kontaktstellen auf die entsprechende DSE hingewiesen werden.	Art. 19 f. nDSG; Art. 13 DSV

5. Betroffenenrechte

Wie nach dem DSG haben betroffene Personen nach dem nDSG bestimmte Rechte (Auskunftsrecht, Berichtigungsrecht, Widerspruchsrecht, Portabilitätsrecht, Anhörungsrecht bei automatisierten Einzelentscheidungen).

Minimalaufgaben:

— Abläufe bei Betroffenenbegehren durchdenken

— ggf. Prozess ggf. in einer Richtlinie festlegen

— sicherstellen, dass Daten gefunden, aufdatiert, extrahiert und gelöscht werden können

— prüfen, ob wesentliche Entscheidungen automatisiert getroffen werden (meistens nicht)

Dokument/Aufgabe	*Anmerkungen*	*Zwingend?*	*Grundlage*
Prozessbeschreibung Umgang mit Betroffenenrechten	Anfragen zur Ausübung von Betroffenenrechten müssen i.d.R. mit einer Frist von 30 Tagen beantwortet werden.	Ein eigener Prozess für den Umgang mit Betroffenenrechten ist sinnvoll, faktisch zwingend aber nur bei komplexen Organisationen oder bei häufigen Betroffenenbegehren. Bei kleineren Organisationen genügt eine Richtlinie oder allgemeine Anweisung; man kann sich auch im Einzelfall rechtlich beraten lassen.	Art. 25 ff. nDSG; Art. 16 ff. DSV
Muster-Korrespondenz	Standard-Texte und Antworten auf Betroffenenanfragen (Hinweise auf Betroffenenrechte bspw. bei der Mitteilung von automatisierten Einzelentscheidungen, Quittierung des Eingangs von Betroffenenbegehren, Nachfrage zur Identifizierung, Ablehnung usw.) sind sinnvoll bei sehr vielen Anfragen oder zur Standardisierung bei einer dezentralen Datenschutzorganisation.	Nein, ausser bei sehr komplexen Organisationen oder sehr häufigen Betroffenenbegehren.	n/a

Prüfung besonderer Anforderungen: Datenportabilität	Nach dem nDSG haben Betroffene das Recht, bestimmte Daten in maschinenlesbarer Form zu verlangen oder jemand anderem direkt übermitteln zu lassen («Datenportabilität»).	Das Portabilitätsrecht besteht bei Daten, die vom Betroffene erhalten wurden oder aus der Erfassung seines Verhaltens stammen. Ggf. müssen solche Daten in einem üblichen Format fristgerecht extrahierbar sein.	Art. 21 nDSG
Prüfung besonderer Anforderungen: automatisierte Einzelentscheidungen	«Automatisierte Einzelentscheidungen» sind Entscheidungen, die automatisiert fallen und für Betroffene erhebliche Auswirkungen haben (z.B. automatische Vertragsablehnung oder Kündigung). Hier bestehen besondere Rechte der Betroffenen.	Bei automatisierten Einzelentscheidungen muss vorab in einer DSE oder im Einzelfall informiert werden, dass die Entscheidung automatisiert erfolgt ist und dass der Betroffene bestimmte Rechte hat.	Art. 21 nDSG

6. Vertragsbestimmungen

Das nDSG sieht in bestimmten Konstellationen eine Pflicht vor, eine bestimmte Form von Verträgen zu schliessen, besonders bei Auftragsbearbeitungen. Es kann strafbar sein, einen Auftragsbearbeiter ohne entsprechenden Vertrag beizuziehen.

Siehe auch Ziff. 4 – Information und Datenschutzerklärungen und Ziff. 7 – Übermittlung ins Ausland

Minimalaufgaben:

— prüfen, wo Auftragsbearbeitungen vorliegen

— entsprechende Verträge prüfen

— bei Bedarf eine Auftragsbearbeitungsvereinbarung abschliessen

Dokument/Aufgabe	*Anmerkungen*	*Zwingend?*	*Grundlage*
Auftragsbearbeitungsvereinbarung (ADV)	I.d.R. ist ein Muster einer ADV erforderlich. Mit bestehenden Auftragsbearbeitern müssen ADV geschlossen werden, soweit eine solche nicht schon vereinbart ist.	Ja. Der Beizug eines Auftragsbearbeiters ohne ausreichende ADV kann strafbar sein.	Art. 9 nDSG, Art. 7 DSV
Vereinbarung zwischen gemeinsam Verantwortlichen	Mehrere Verantwortliche können gemeinsam verantwortlich sein, wenn sie arbeitsteilig zusammenwirken. Eine Vereinbarung kann die Zuständigkeiten und Verantwortlichkeiten für den Datenschutz klarstellen.	Nein, nicht nach schweizerischem Recht, aber eine solche Vereinbarung ist oft sinnvoll. Sie erleichtert auch eine korrekte Beantwortung von Betroffenenbegehren.	n/a
Standardklauseln in AGB und anderen Vertragsunterlagen	Hinweis auf die relevante DSE (i.d.R. die allgemeine DSE auf der Website) in AGB und in anderen Vertragsunterlagen (Antragsformularen usw.). Allenfalls auch Musterklauseln in Einkaufs- oder Lieferbedingungen und weiteren Verträgen.	Nein, nicht nach schweizerischem Recht, aber zumindest in Vertragsunterlagen für Endkunden drängen sich solche Verweisungen auf.	n/a

Vertraulichkeitsvereinbarungen mit Dritten	Standardisierte Vertraulichkeitsklauseln oder Vertraulichkeitsvereinbarungen («NDA») mit Dritten, die Personendaten und/oder geheime Daten erhalten.	Ja, wenn Personendaten und besonders wenn geheime Daten an Drittempfänger (d.h. nicht Auftragsbearbeiter) bekanntgegeben werden, müssen die Vertraulichkeit und die Zweckbindung beim Dritten sichergestellt werden.	Art. 6-8 und 62 nDSG; Art. 321 StGB usw.

7. Übermittlung ins Ausland

Das nDSG begrenzt wie das heutige DSG die Bekanntgabe von Personendaten ins Ausland, wenn im Empfängerstaat kein angemessenes Datenschutzniveau herrscht. Diese Länder ergeben sich aus einer Liste im Anhang der DSV. Wenn keine Ausnahme gilt, muss für eine solche Bekanntgabe eine bestimmte Art von Vereinbarung mit dem Empfänger geschlossen werden. Bei einer Bekanntgabe ins Ausland sind zudem ggf. Auftragsbearbeitungsverträge oder andere Datenschutzvereinbarungen erforderlich (siehe Ziff. 6 – Vertragsbestimmungen).

Minimalaufgaben:

— prüfen, wo Daten ins Ausland bekanntgegeben werden bzw. gelangen

— prüfen, ob die entsprechenden Länder ausserhalb des EWR liegen; entsprechende Verträge prüfen und bei Bedarf die Standardvertragsklauseln mit den EDÖB-Anpassungen für die Schweiz vereinbaren

— in diesem Fällen ein «Transfer Impact Assessment» durchführen (lassen)

Dokument/Aufgabe	*Anmerkungen*	*Zwingend?*	*Grundlage*
Verwendung der EU-Standardvertragsklauseln	Ein von der EU und der Schweiz anerkanntes Vertragswerk («SCC»), das die Übermittlung in Staaten ohne angemessenes Schutzniveau (z.B. die USA, Indien oder China; «Drittstaat») legitimieren kann. Die SCC müssen punktuell an schweizerisches Recht angepasst werden.	Ja, sofern keine Ausnahme oder andere Grundlage für die Übermittlung greift. Die Übermittlung von Personendaten in solche Staaten ohne ausreichende Absicherung kann strafbar sein.	Art. 16 f. und Art. 61 nDSG; Art. 9 f. DSV
Anpassung bestehender Verträge	Soweit Verträge mit Empfängern in einem Drittstaat keine oder die alten SCC verwendet, müssen diese Verträge so rasch wie möglich angepasst werden.	Ja, soweit solche Verträge bestehen. Das ist ggf. zu prüfen.	Art. 16 f. und Art. 61 nDSG; Art. 9 f. DSV
«Transfer Impact Assessment»	Die SCC binden nur den Empfänger, aber nicht die lokalen Behörden. Diese können auf der Grundlage des lokalen Rechts u.U. auf übermittelte Personen-	Ja. Die SCC dürfen nur verwendet werden bzw. genügen nur dann, wenn ein Transfer Impact Assessment ergeben hat, dass das Restrisiko inakzeptabler Behördenzugriffe ausreichend niedrig ist.	Art. 16 f. und Art. 61 nDSG; Art. 9 f. DSV

	daten zugreifen. Um das Risiko von aus schweizerischer Sicht inakzeptablen Zugriffen zu beurteilen, muss es eingeschätzt werden, in der Regel durch ein sogenanntes «Transfer Impact Assessment».	Das gilt besonders auch dann, wenn geheime Daten ins Ausland übermittelt werden.	

8. Compliance- und Risikoprüfungen

Das schweizerische Recht schreibt nicht vor, dass Bearbeitungsprozesse proaktiv zu prüfen sind, aber wenn die Bearbeitungsgrundsätze nicht eingehalten werden, ist das eine Datenschutzverletzung. Bei Bearbeitungen, die voraussichtlich ein hohes Risiko mit sich bringen, muss zudem eine «Datenschutz-Folgenabschätzung» vorgenommen werden.

Minimalaufgaben:

— überlegen, ob die Datenbearbeitungen die Grundsätze einhalten, vor allem, ob möglichst wenige Daten möglichst weniger Personen möglichst kurz gespeichert und möglichst wenigen Personen zugänglich gemacht werden und ob Daten nur so verwendet werden, wie es ursprünglich mitgeteilt wurde oder zu erwarten war

— je nachdem Korrekturmassnahmen ergreifen

— überlegen, ob die Voraussetzungen für eine Datenschutz-Folgenabschätzung (DSFA) vorliegen

— ggf. eine DSFA durchführen

Dokument/Aufgabe	*Anmerkungen*	*Zwingend?*	*Grundlage*
Prüfung aller Prozesse auf Konformität und Risiken	Allgemeine Prüfung bei allen Bearbeitungen auf Einhaltung der datenschutzrechtlichen Anforderungen (besonders der Bearbeitungsgrundsätze) und auf hohe Risiken	Nein, das schweizerische Recht verlangt eine solche Prüfung und Dokumentation nicht (aber natürlich muss der Datenschutz eingehalten werden).	n/a
Datenschutz-Folgenabschätzung («DSFA»)	Strukturierte Prüfung der Risiken einer Bearbeitungstätigkeit für betroffene Personen. Sinnvoll ist die Verwendung einer Vorlage.	Ja, sofern eine Bearbeitung voraussichtlich ein hohes Risiko für Betroffene mit sich bringt, besonders wenn besonders schützenswerte Personendaten (z.B. Gesundheitsdaten) umfangreich bearbeitet werden, wenn umfangreiche öffentliche Bereiche systematisch überwacht werden und bei einem Profiling mit hohem Risiko. Die DSFA ist mindestens zwei Jahren nach Beendigung der Datenbearbeitung aufzubewahren.	Art. 22 nDSG; Art. 14 DSV

9. Daten von Mitarbeitenden

Im Arbeitsbereich werden Personendaten in grösserem Umfang bearbeitet, die Personen in einer gewissen Abhängigkeit betreffen. Hier bestehen zudem auch zusätzliche Rechtsrisiken für Unternehmen, aufgrund häufiger Ansprüche von Mitarbeitenden. Der Datenschutz in diesem Bereich ist deshalb besonders wichtig, auch für Unternehmen, die im B2B-Bereich ansonsten kaum Personendaten bearbeiten.

Minimalaufgaben:

— eine DSE für Mitarbeitende ausarbeiten und abgeben

— DSE für Stellenbewerbende ausarbeiten

— überlegen, ob bei Mitarbeiterdaten die Bearbeitungsgrundsätze einhalten werden (siehe Ziff. 8 – Compliance- und Risikoprüfungen)

— siehe auch Ziff. 11 – Datenlöschung

Dokument/Aufgabe	*Anmerkungen*	*Zwingend?*	*Grundlage*
Datenschutzerklärung – Mitarbeitende	Eine DSE für Mitarbeitende erläutert den Umgang mit Daten von Mitarbeitenden ab Einstellung.	Ja, eine DSE für Mitarbeitende ist zwingend. Sinnvoll ist eine Verweisung darauf im Arbeitsvertrag oder Personalreglement.	Art. 19 f. und Art. 61 nDSG; Art. 13 DSV
Datenschutzerklärung – Stellenbewerbende	Eine DSE für Bewerbende erläutert den Umgang mit Daten von Bewerbenden bis zur Einstellung bzw. im Fall einer Ablehnung.	Ja, es sei denn, die Bearbeitung solcher Daten wird in der DSE für Mitarbeitende eingeschlossen, was oft aber nicht der Fall ist. Sinnvoll kann auch ein Datenschutzhinweis in einem Standard-Antwortschreiben auf Bewerbungen sein.	Art. 19 f. und Art. 61 nDSG; Art. 13 DSV
Geheimhaltungsvereinbarungen mit Mitarbeitenden	Ausdrückliche Geheimhaltungsbestimmung im Arbeitsvertrag, im Arbeitsreglement oder in einem separaten Dokument.	Nein, aber vor allem dann sinnvoll, wenn das Unternehmen gegenüber Dritten Vertraulichkeitsvereinbarungen schliesst oder Daten bearbeitet, die einem Berufsgeheimnis unterliegen.	n/a (Art. 321a Abs. 4 OR; Art. 321 StGB usw.)

10. Datensicherheit

Das nDSG und die DSV setzen einen Rahmen für die Mindestsicherheit von Personendaten. Es ist unklar, welche dieser Massnahmen strafrechtlich relevant sind. Es besteht daher ein Strafbarkeitsrisiko, wenn die Sicherheit nicht eingehalten wird. Dazu kann bei heiklen Bearbeitungen auch eine Protokollierung diverser Vorgänge einschliesslich des Lesens von Daten gehören.

Minimalaufgaben:

— prüfen, ob die verwendeten IT-Systeme bzw. Komponenten ausreichend sicher sind bzw. mit der IT prüfen, welche Standards und Prozesse dafür bestehen und ob sie auf dem aktuellen Stand sind

— überlegen, ob die Voraussetzungen für eine Protokollierungspflicht erfüllt sind

— Umgang mit Sicherheitsverletzungen durchdenken, ggf. Prozess aufschreiben und mit den betreffenden Personen oder Funktionen durchspielen

Dokument/Aufgabe	*Anmerkungen*	*Zwingend?*	*Grundlage*
Gewährleistung der Datensicherheit	Das nDSG verlangt, dass Personendaten angemessen gegen Verlust, Beschädigung und Zugriff geschützt werden. Dazu sind geeignete technische und/oder organisatorische Massnahmen zu treffen (z.B. Schutz der IT-Systeme und physischen Infrastruktur, Absicherung des need-to-know-Grundsatzes bei Konfiguration und Verwaltung der IT, Verhinderung von Zugriffen und Änderungen gespeicherter Daten, Schutz bei Übermittlung, Wiederherstellbarkeit von Daten, Updates der Systeme und Applikationen, Nachvollziehbarkeit von Zugriffen und Änderungen und Umgang mit Verletzungen). Das sollte dokumentiert werden.	Ja. Eine Verletzung der Datensicherheit kann u.U. strafbar sein (strittig).	Art. 8 nDSG; Art. 1 ff. DSV
Protokollierung	In bestimmten Fällen müssen Verantwortliche und Auftragsbearbeite das Speichern, Verändern, Lesen	Ja, wenn besonders schützenswerte Personendaten in grossem Umfang automatisiert bearbeitet werden oder	Art. 4 DSV

	(!), Bekanntgeben, Löschen und Vernichten protokollieren. Zu erfassen ist dabei, wer wann welche Bearbeitungen vorgenommen hat und ggf. wem Daten bekanntgegeben werden. Protokolle müssen während mindestens einem Jahr getrennt vom produktiven Systemaufbewahrt werden.	ein Profiling mit hohem Risiko durchgeführt wird, andere Massnahmen den Datenschutz aber nicht gewährleisten.	
Prozess zum Umgang mit Sicherheitsverletzungen	Wenn der Schutz von Personendaten kompromittiert wurde (wenn Daten versehentlich oder aufgrund eines Angriffs von aussen oder innen verlorengehen, gelöscht, vernichtet oder verändert werden oder offengelegt werden), muss die Verletzung dem EDÖB gemeldet werden, falls sie voraussichtlich zu hohen Risiken für die Betroffenen führt; und den Betroffenen mitgeteilt werden, wenn das zu ihrem Schutz notwendig ist. Zudem müssen die Verletzung, ihre Auswirkungen und die ergriffenen Massnahmen dokumentiert werden. Die Dokumentation muss dem Zeitpunkt der Meldung zwei Jahre aufbewahrt werden. Auftragsbearbeiter müssen den Verantwortlichen über Verletzungen informieren.	Faktisch meist ja, weil Sicherheitsverletzungen häufig sind eine Verletzung der Melde- bzw. Mitteilungspflicht eine Datenschutzverletzung ist, auch wenn sie nicht strafbar ist.	Art. 22 und 24 Abs. 3 nDSG; Art. 15 DSV

11. Datenlöschung

Personendaten dürfen nur aufbewahrt werden, solange es für die Bearbeitung oder die Einhaltung gesetzlicher Aufbewahrungspflichten notwendig ist. Werden sie anschliessend nicht gelöscht oder anonymisiert, stellt dies eine Verletzung dar und erhöht generell Risiken für das Unternehmen wie auch Betroffene. Die Sicherstellung der Löschung ist eine schwierige und meist langwierige Aufgabe.

Minimalaufgaben:

— überlegen, ob Daten gelöscht werden und ob bekannt ist, welche Aufbewahrungsfristen gelten

— ggf. Fristen bestimmen

— Löschprozess installieren oder ggf. regelmässig händisch löschen

Dokument/Aufgabe	*Anmerkungen*	*Zwingend?*	*Grundlage*
Gewährleistung einer rechtzeitigen Datenlöschung	Personendaten dürfen grundsätzlich nur solange aufbewahrt werden, wie es für die Zwecke der Bearbeitung oder für Aufbewahrungspflichten notwendig ist. Anschliessend müssen sie gelöscht oder anonymisiert werden.	Ja. Eine zu lange Speicherung ist eine Datenschutzverletzung, erhöht die Risiken bei Sicherheitsverletzungen und erschwert den Umgang mit Betroffenenrechten.	Art. 6 Abs. 2-4 nDSG
Bestimmung von Aufbewahrungs- bzw. Löschfristen	Für eine regelmässige Datenlöschung müssen Aufbewahrungsfristen pro Datenkategorie festgelegt werden. Dabei können unterschiedliche Aufbewahrungspflichten gelten.	Ja. Eine zu späte Löschung ist datenschutzwidrig (s. oben), eine zu frühe Löschung kann Aufbewahrungsfristen verletzen.	Diverse Bestimmungen im Bereich HR, Steuern, Handelsrecht usw.
Definierte Löschprozesse (übergreifend oder applikationsspezifisch)	Eine regelkonforme Löschung setzt nicht nur die Bestimmung der Aufbewahrungsfristen voraus, sondern auch löschfähige Systeme und eine entsprechende Systemkonfiguration.	Faktisch meist ja, eine händische Löschung ist illusorisch.	Art. 6 Abs. 2-4 nDSG