walderwyss rechtsanwälte

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 DSG und DSGVO

Umsetzung der datenschutzrechtlichen Compliance

V015

Das revidierte Datenschutzgesetz der Schweiz («nDSG») wurde am 25. September 2020 verabschiedet und tritt zusammen mit der revidierten Verordnung zum DSG («DSV») **per 1. September 2023** in Kraft.

Die Umsetzung des nDSG verlangt eine gewisse Planung. Sie ist nur effektiv, wenn sie der Tätigkeit und Struktur sowie den Risiken und Bedürfnissen des Unternehmens Rechnung trägt – *one size fits all* ist hier ein falscher Ansatz. Die Umsetzung muss vielmehr auf die **konkreten Umstände** Rücksicht nehmen. Dazu gehören der Umfang und die Komplexität der Geschäftstätigkeiten des bzw. der Unternehmen, die Bedeutung von Datenbearbeitungen für das Geschäftsmodell, aber auch die Sensitivität der bearbeiteten Personendaten und die Anwendbarkeit regulatorischer bzw. sektorieller datenrechtlicher Bestimmungen. Von Bedeutung ist auch, welchen Stellenwert die Reputation für das Unternehmen besitzt und welche Erwartungen aufseiten des Publikums und der Behörden bestehen. Schliesslich ist zu beachten, wie komplex die IT-Landschaft des Unternehmens gestaltet und wie es um die bestehenden Prozesse und ihre Dokumentation bestellt ist – insbesondere in den Bereichen Warenproduktion, Leistungen und Vertrieb, IT, HR und Marketing.

«Compliance» ist kein Selbstzweck, sondern die Vorgabe, Risiken für die betroffenen Personen zu erkennen, zu verstehen und angemessen und bewusst damit umzugehen. Das ist eine Daueraufgabe.

Dieses Dokument ist auch auf Englisch und Französisch verfügbar.

Die **ersten und wichtigsten Schritte** sind oft mit wenig Aufwand möglich. Das gilt besonders dann, wenn bereits Umsetzungsarbeiten für die EU-Datenschutzgrundverordnung («DSGVO») erfolgt sind. In diesem Dokument finden sich deshalb Hinweise auf die wichtigsten Schritte für Unternehmen, die bei der Umsetzung am Anfang stehen, und auf Arbeiten, die bei einer bereits erfolgten Umsetzung der DSGVO ergänzend erforderlich sind.

Unternehmen, die mit der Umsetzung der DSGVO bzw. des nDSG beginnen, empfehlen wir folgende Erst- bzw. Mindestmassnahmen:

1. Prüfung der anwendbaren rechtlichen Bestimmungen
2. Ausarbeitung einer Datenschutz-Richtlinie
3. Aufnahme von Bearbeitungsverzeichnissen
4. Ausarbeitung von Datenschutzerklärungen für Produkte/Leistungen, die Website bzw. für Apps, Mitarbeiter und evtl. für Stellenbewerber
5. Gewährleistung einer ausreichenden, den Risiken angemessenen Datensicherheit
6. Ausarbeitung einer Auftragsbearbeitungsvereinbarung für Kunden, soweit das Unternehmen im IT-Bereich Dienstleistungen erbringt oder sonst als Auftragsbearbeiter von Kunden tätig ist

Wir helfen mit einer umfangreichen Toolbox aus Anleitungen, Checklisten und Vorlagen, den Aufwand und Zeitbedarf wie auch die Kosten zu kontrollieren und zu reduzieren.

Planungsfragen

Die Umsetzung der DSGVO und des nDSG ist nicht unbedingt aufwendig, verlangt aber eine gewisse Planung – schon aus Gründen der Budgetierung und des Reportings. Als Planungshilfe sind Checklisten usw. verfügbar. Wichtig ist nicht Vollständigkeit, sondern eine konkrete Vorstellung des vom Vorgehen, damit auf Änderungen und Verzögerung richtig reagiert werden kann.

1 *Projektumfang und -gegenstand*

Das Umsetzungsprojekt und dessen Umfang und Gegenstand sind zu planen. Hier lauten die Kernfragen etwa, ob man es mit einer (teil-)konzernweiten Umsetzung oder einzelnen Gesellschaften zu tun hat, ob nur gesamthafte Beteiligungen oder auch Mehr- und Minderheitsbeteiligungen einzubeziehen sind und ob die Konzerngesellschaften zwingend daran partizipieren oder bloss über Empfehlungen und Hilfestellungen eingebunden werden. Sodann sind die bereits erfolgten Umsetzungsarbeiten auf Basis der DSGVO oder des DSG zu berücksichtigen und die Projektziele samt Erfolgsmessung zu bestimmen.

Bei abgeschlossener DSGVO-Umsetzung: Bestimmung des Anpassungsaufwands bestehender Dokumente und Prozesse

Was den Zeitplan betrifft, treten das **nDSG** und die DSV am 1. September 2023 in Kraft. Beide enthalten nur eingeschränkte Übergangsfristen, die meisten Anforderungen gelten direkt mit dem Inkrafttreten.

Bei **kleineren Unternehmen** ohne hochriskante Bearbeitungen von Personendaten und ausserhalb des Geltungsbereichs der DSGVO ist die Umsetzung i.d.R. weder zeitaufwendig noch kostenintensiv.

2 *Umsetzungsvorgaben*

1 Erstmassnahme

Wichtig ist die Prüfung des relevanten rechtlichen Rahmens, der die Projektziele mit vorgibt. Dies betrifft zum einen die DSGVO und ggf. auch deren Umsetzungsrecht, aber auch die Gruppenvorgaben wie etwa die Einhaltung der DSGVO.

Weiter ist zu prüfen, wieweit das nDSG anwendbar ist, namentlich in Bezug auf die internationale Ebene (Territorialität- und Auswirkungsprinzip) sowie die Bestimmungen über Bundesorgane. Schliesslich werfen sektorielle Bestimmungen (in der Schweiz und/oder im Ausland) die Frage nach der freiwilligen Anwendbarkeit strengerer Regelungen und deren Umfang auf.

Bei abgeschlossener DSGVO-Umsetzung: Bestimmung weiterer Anforderungen, die bei der DSGVO-Umsetzung ggf. nicht berücksichtigt worden sind, und Entscheidung über eine freiwillige Umsetzung der DSGVO (zusammen mit dem nDSG) in der Schweiz

Das **Umsetzungsrecht enthält z.T. strengere Anforderungen**, besonders in regulierten Bereichen (ggf. auch strafbewehrte Berufsgeheimnisse). Diesbezüglich kann es sich anbieten, die Anwendbarkeit der DSGVO aktiv auszuschliessen (z.B. durch Ausschluss von Kunden aus dem EWR oder des Trackings bei Besuchern aus dem EWR).

Eine **freiwillige Anwendung** der DSGVO ist demgegenüber oft sinnvoll bei einer Eingliederung in einen ausländischen Konzern, bei Dienstleistern mit ausländischen Kunden und bei Anbietern mit erheblichem Kundenstamm im Ausland. Die freiwillige Anwendung ist dabei oft beschränkt (und führt daher bspw. nicht zu Einwilligungserfordernissen, die das nDSG nicht kennt).

3	*Projektvorgehen*	Ebenfalls entscheidend ist, das konkrete Vorgehen im Projekt zu planen. Das Vorgehen gestaltet sich je nach den Umständen unterschiedlich. Besonders zu beachten ist die Frage, ob man eine zentrale Steuerung anstrebt oder es bei Hilfestellungen und Ressourcen für die einzelnen Gesellschaften bzw. Bereiche bewenden und sie auch die Verantwortung für die Umsetzung tragen lässt. Die wichtigsten Hilfsangebote müssen geplant und das interne Projektsponsoring sowie allfällige externe Unterstützung bestimmt werden. Hinzu kommen zeitliche Vorgaben sowie die Budgetierung, das Controlling und Reporting.	

Funktionen und Verantwortlichkeiten

Die Datenschutz-Compliance als laufende Aufgabe verlangt eine der Grösse und Komplexität des Unternehmens angemessene Struktur und die notwendigen Kompetenzen. Eine eigene Fachstelle oder Funktion für den Datenschutz ist aber nicht rechtlich zwingend, mit Ausnahme der Bestellung eines Datenschutzbeauftragten («DPO») im Anwendungsbereich der DSGVO bei bestimmten, heikleren Datenbearbeitungen. Das nDSG kennt keinen DPO, sieht aber einen Datenschutzberater vor, dessen Bestellung immer freiwillig ist.

Sowohl die DSGVO als auch das nDSG sehen zudem, unter bestimmten Voraussetzungen, eine lokale Vertretung eines Unternehmens ausserhalb des EWR bzw. der Schweiz vor.

4	*Gruppeninterne Funktionen*	Zentrale Funktionen, deren Kompetenzen und Verantwortlichkeiten sowie deren Rolle bei der Umsetzung sind zu planen. Neben einer eigenen Fachstelle für Datenschutz kommen eigene Datenschutzkompetenzen im Legal- und Compliance-Bereich in Betracht sowie die Schaffung von Datenschutz-Champions oder ähnlichen Funktionen in Gruppengesellschaften bzw. Bereichen. Die Wahl ist abzustimmen auf die Komplexität und den Zentralisierungsgrad sowie die verfügbaren Kompetenzen und Kapazitäten.	**Bei abgeschlossener DSGVO-Umsetzung**: Prüfung der Kompetenzen in den Gruppenfunktionen bzgl. des nDSG, soweit erforderlich, oder Aufbau einer Beziehung zu externen Beratern
5	*Datenschutzbeauftragter (DPO i.S.d. DSGVO)*	Zu prüfen ist, ob ein **Datenschutzbeauftragter** («DPO») nach der DSGVO bestellt werden muss oder soll. Dies bestimmt sich nach der DSGVO und dem lokalen Umsetzungsrecht, das, wie z.B. in Deutschland, teils strengere Anforderungen kennt. Neben der Auswahl und dem Bestellvorgang des DPO muss das Reporting geplant und die Rollen und Verantwortlichkeiten klar definiert	**Bei abgeschlossener DSGVO-Umsetzung**: Bestellung des DPO als Datenschutzberater prüfen (s. unten, Ziff. 6)

werden. Dies macht ggf. auch Anpassungen im Bearbeitungsverzeichnis, der DSE sowie bei bestehenden Prozessen nötig. Konkret ist z.B. der Einbezug des DPO z.B. bei Datenschutz-Folgenabschätzungen («DSFA») festzulegen.

Eine **externe Stelle** kann als DPO bestellt werden, wobei nach nicht unumstrittener Praxis auch juristische Personen dafür in Frage kommen.

6 *Datenschutzberater (i.S.d. nDSG)*

Eine Bestellungspflicht besteht nach dem nDSG nicht. Dennoch kann sich besonders bei Unternehmen mit heikleren Bearbeitungen eine **freiwillige Bestellung** lohnen. Auch hier ist darauf zu achten, dass neben der Auswahl und dem Bestellvorgang des Beraters das Reporting geplant und die Rollen und Verantwortlichkeiten klar definiert werden. Dies macht ggf. auch Anpassungen im Bearbeitungsverzeichnis, der DSE sowie bei bestehenden Prozessen nötig.

Konkret ist z.B. der Einbezug des Beraters bei **Datenschutz-Folgenabschätzungen** («DSFA») festzulegen. Obschon dessen Bestellung freiwillig ist, befreit sie bei korrekter Bestellung von der Pflicht, dem EDÖB hohe Nettorisiken bei der DSFA zu melden (vgl. Ziff. 21).

Bei abgeschlossener DSGVO-Umsetzung: ggf. Bestellung eines unabhängigen Datenschutzberaters

Bestimmte Anforderungen gelten hinsichtlich der **Unabhängigkeit**: Der Datenschutzberater sollte keine Exekutivfunktionen innehaben. Eine Personalunion mit dem DPO ist möglich, wenn der DPO über ausreichende Kenntnisse verfügt oder darauf zugreifen kann.

Auch eine **externe Stelle** – und darunter auch juristische Personen – kommen als Berater in Frage.

7 *EU- und UK-Vertreter*

Bei Unternehmen, die unter die DSGVO fallen, im EWR bzw. im Vereinigten Königreich aber keine Niederlassung haben, ist der EU- bzw. UK-Vertreter ist eine lokale Ansprechperson für Behörden und betroffene Personen. Auch hier gilt es, die Bestellungspflicht zu prüfen. Im Falle einer Bestellung sind Anpassungen in der DSE sowie im Bearbeitungsverzeichnis und dessen Prozessen vorzunehmen, etwa den Erhalt von Kopien zuhanden des EU-Vertreters.

Bei abgeschlossener DSGVO-Umsetzung: ggf. Bestellung eines EU-Vertreters

Eine Bestellungspflicht besteht, wenn die DSGVO nach Art. 3 Abs. 2 anwendbar ist (d.h. bei Marktausrichtung oder Verhaltensbeobachtung), sofern die entsprechende Verarbeitung nicht nur gelegentlich erfolgt und/oder besondere Datenkategorien umfangreich bearbeitet werden und/oder die Bearbeitung zu einem erhöhten Risiko führt.

Der EU-Vertreter muss sich in einem EWR-Staat befinden, in dem sich angesprochene oder beobachtete Personen befinden. Er kann eine natürliche oder juristische Person sein. Dasselbe gilt für das Gebiet des Vereinigen Königreichs nach der UK GDPR.

8 *CH-Vertreter*

Der CH-Vertreter ist ebenfalls eine lokale Ansprechperson für den EDÖB und betroffene Personen in der Schweiz. Er ist auf Unternehmen mit ausländischem Sitz zugeschnitten, die unter das nDSG fallen.

Bei abgeschlossener DSGVO-Umsetzung: ggf. Bestellung eines CH-Vertreters (z.B. eine Gruppengesellschaft mit Niederlassung in der Schweiz)

Auch hier ist die Bestellungspflicht zu prüfen. Eine Bestellung macht Anpassungen der DSE erforderlich, aber nicht unbedingt des Bearbeitungsverzeichnisses. Eine Bestellungspflicht besteht bei einem Sitz des Verantwortlichen im Ausland und unter folgenden Voraussetzungen: (i) Bearbeitung von Daten von Personen in der Schweiz; die Bearbeitung steht (ii) im Zusammenhang mit Angeboten an diese Personen oder der Beobachtung ihres Verhaltens; sie ist (iii) **umfangreich und regelmässig** und ist (iv) **hochriskant** für die betroffenen Personen.

Der CH-Vertreter kann eine natürliche oder juristische Person sein, auch eine Konzerngesellschaft in der Schweiz oder ein externer Dienstleister.

Dokumentation

Nach der DSGVO muss der Verantwortliche nachweisen können, dass und wie er die DSGVO einhält (Stichwort «Accountability»). Ein Verstoss ist sanktionsbedroht. Das nDSG kennt keine solche Accountability-Pflicht, eine Dokumentation ist in einem bestimmten Umfang aber gleichwohl notwendig, besonders in Form sog. «Bearbeitungsverzeichnisse».

9 *Dokumentation im Allgemeinen*

Sinnvoll und u.U. zwingend ist eine **zentrale Erfassung** datenschutzrelevanter Handlungen und Ereignisse.

Dazu zählen etwa Bearbeitungsverzeichnisse, Richtlinien und weitere Dokumentation, die Prüfung eines berechtigten Interesses («legitimate interest assessments», LIAs), DSFA und Folgehandlungen, Datenschutzverletzungen und Reaktionen, die Verweisung auf Sicherheitsmassnahmen (TOMs), Drittparteien und Contract Management, Betroffenenanfragen (alle/eskalierte), gruppeninterne Auftragsbearbeitungs-, Joint Controller- und Drittbekanntgabeverhältnisse, Datenbekanntgaben in Drittstaaten, ggf. mit Risikoeinschätzung («Transfer Impact Assessment», «TIAs»; siehe Ziff. 28), das Reporting und Empfehlungen des DPO/Datenschutzberaters, die Verweisung auf Drittparteien/Contract Management sowie Behördenkontakte.

Diese Dokumentation kann in unterschiedlicher Weise geführt werden, so z.B. in einem Exceldokument, in einem Dokument über Sharepoint, allenfalls auch in einem Bereich des Intranets, ferner über OneTrust, Confluence etc. Dabei sollte die Dokumentation nutzerfreundlich sein und eine Kontrolle der Zugriffsberechtigungen ermöglichen.

Das nDSG kennt keine eigentliche Accountability-Pflicht. Eine gewisse Dokumentation ist aber dennoch notwendig, als Teil der Governance, aber auch aus Beweisgründen.

10 *Regelwerke, Policies, Anleitungen*

2 Erstmassnahme

Aus der Accountability-Pflicht, aber auch im Sinne einer Datensicherheitsmassnahme und als Teil der Verantwortung des Unternehmens und seiner Leitungsorgane sind bestimmte Vorgaben notwendig. Dabei sind die Umstände massgebend und unnötige Vorgaben zu vermeiden. Als Massnahmen kommen **Datenschutz-Policies** wie z.B. ein Code of Conduct oder eine Richtlinie in Frage, ggf. auch abgeleitete Policies, Leitfäden, Merkblätter, Umsetzungshilfen etc.

Typische Beispiele sind Vorgaben im IT-Bereich, wie sie oft bereits bestehen und etwa die erlaubte Nutzung oder das Monitoring regeln, aber auch Videoüberwachungen, der Einsatz von Cloud-Diensten, HR-Vorgaben wie BYOD; CRM- und Marketingtools und Betroffenenrechte.

Entsprechende Dokumente sind auf den Bedarf abzustimmen und nur zu entwerfen, wenn sie notwendig sind und gepflegt werden (siehe Ziff. 15). Schliesslich ist die Umsetzung, etwa ein internes Sign-Off oder Ausrollen, zu planen.

Bei abgeschlossener DSGVO-Umsetzung: Prüfung und ggf. Anpassung bestehender Regelwerke

Abweichungen zu Regelwerken, die auf die DSGVO ausgerichtet sind, sind sehr wahrscheinlich. Erforderlich ist eine **Prüfung und ggf. eine Anpassung** an die Schweiz bzw. an das nDSG.

Erforderlich ist auch eine formale Inkraftsetzung durch die für schweizerische Unternehmen zuständigen Organe bzw. Stellen.

Bearbeitungsverzeichnisse und Bearbeitungsreglement

Das Bearbeitungsverzeichnis ist ein Inventar, in dem die unterschiedlichen Datenbearbeitungen mit bestimmten Mindestangaben erfasst werden. Es ist sowohl nach der DSGVO als auch nach dem nDSG zwingend, sofern nicht Ausnahmen greifen. Erfasst werden nicht Applikationen oder einzelne Personendaten, sondern die unterschiedlichen Zwecke der Bearbeitung und ihre wesentlichen Rahmenbedingungen.

11 *Technische Umsetzung*

Besonders bei grösseren Unternehmen oder vielfältigen Bearbeitungen ist es sinnvoll, auf eine **nutzerfreundliche Umsetzung** der Verzeichnisse zu achten. Zu bestimmen ist daher die technische Umsetzung der Bearbeitungsverzeichnisse und ihrer Erhebung (vgl. Ziff. 9).

Bei abgeschlossener DSGVO-Umsetzung: Verwendung der bestehenden Systeme

12 *Inhalt, Gestaltung, Umfang*

Bei der **Ausgestaltung** ist – neben dem vorgeschriebenen Mindestinhalt – auf Schnittstellen zu anderen Verzeichnissen zu achten, wie etwa das Applikationsverzeichnis oder diejenigen von Drittparteien. Bezüglich Umfang ist zu entscheiden, ob der Mindestinhalt genügt oder weitere Punkte mitaufgenommen gehören wie bspw. eine Schwellenwertbeurteilung für DSFA durch Risikofragen.

Die Ausgestaltung hängt schliesslich davon ab, ob ein **Verantwortlicher** oder ein **Auftragsbearbeiter** das Verzeichnis führt.

Bei abgeschlossener DSGVO-Umsetzung: Verwendung der bestehenden Vorlagen und Prozesse

13 *Initiale Erstellung*

3 Erstmassnahme

An dieser Stelle sind die erforderlichen Prozesse zu planen, also die Zuständigkeiten, die Verantwortlichkeit für Inhalte, Vorgehen und Dokumentation, der Einbezug des DPO bzw. Datenschutzberaters, ferner die Validierung, zeitliche Vorgaben und die Dokumentierung des EU- oder CH-Vertreters mit Kopien.

Bei Bedarf sind auch **Hilfestellungen** vorzubereiten wie Schulungen, Muster typischer Verzeichnisse, schriftliche Anleitungen und Interviews.

Bei abgeschlossener DSGVO-Umsetzung: Initiale Erhebung entlang bestehender Prozesse, mit Anpassungen gemäss Zuständigkeiten und Kapazitäten in der Schweiz

Auch das nDSG kennt eine **Pflicht zur Erhebung** der Bearbeitungen in einem Verzeichnis. Die Verletzung ist nicht direkt sanktioniert, aber es drohen Beweisprobleme, eine faktische Beweislastumkehr bei Verstössen und eine strengere Prüfung bei anderen Verstössen.

Der DSGVO-Standard erfüllt auch die Anforderungen des nDSG. Zu beachten sind allerdings die Ausnahme der Erstellungspflicht für **KMU**. Bundesorgane müssen Bearbeitungsverzeichnisse an den EDÖB melden.

14 *Laufende Erstellung*

Ebenso wichtig wie die initiale Erhebung der Verzeichnisse ist die **laufende Erhebung** neuer Bearbeitungsarten. Zu denken ist hier an die Prüfung des Auslösers (neue Bearbeitungen, bestimmte Änderungen bestehender Bearbeitungen) und die Planung der entsprechenden Prozesse (Zuständigkeiten, Verantwortlichkeit für Inhalte, Vorgehen, Dokumentation, Einbezug des DPO bzw. Datenschutzberaters, Kopien an EU-/CH-Vertreter).

Darüber hinaus sind wiederum Schnittstellen zu anderen Prozessen zu beachten bzw. solche Schnittstellen in diesen Prozessen zu verankern, bspw. die Projektgenehmigung oder Budgetierung.

Bei abgeschlossener DSGVO-Umsetzung: Verwendung der etablierten Prozesse

Auch hier ist die KMU-Ausnahme (siehe Ziff. 13) zu beachten.

15 *Aufrechterhaltung*

Bestehende Verzeichnisse sind grundsätzlich à jour zu halten. Dafür besteht keine konkrete Vorgabe, aber ein Prozess zur regelmässigen Überprüfung von Verzeichnissen (z.B. in bestimmten Intervallen oder nach einem bestimmten Muster, i.d.R. durch die business-

Bei abgeschlossener DSGVO-Umsetzung: Verwendung der etablierten Prozesse

seitig letztverantwortliche Stelle) ist sinnvoll, ebenso wie Stichproben, insbesondere bei heikleren Bearbeitungen.

16 *Bearbeitungsreglemente*

Neben dem Bearbeitungsverzeichnis sehen das nDSG bzw. die DSV vor, dass Verantwortliche und Auftragsbearbeiter für automatisierte Bearbeitungen ein Bearbeitungsreglement erstellen müssen, soweit sie besonders schützenswerte Personendaten in grossem Umfang bearbeiten oder ein Profiling mit hohem Risiko durchführen. Für Bundesorgane sind die entsprechenden Vorschriften strenger. Das Bearbeitungsreglement soll einen Überblick über die Massnahmen zur Gewährleistung des Datenschutzes geben und kann ggf. auf bestehende Dokumente – wie z.B. eine Liste vom TOMs – verweisen.

Es ist zu prüfen, ob die Voraussetzungen für die Pflicht zur Erstellung eines Bearbeitungsverzeichnisses gegeben sind und, falls dem so ist, ob bereits einschlägige Dokumentationen bestehen, auf die verwiesen werden kann. Auch in diesem Fall ist aber ein Bearbeitungsreglement zu erstellen, das sich grundsätzlich auch ein Deckblatt mit Angabe der vorhandenen Dokumentation beschränken kann.

Transparenz, Information und Einwilligungen

Sowohl die DSGVO als auch das nDSG verlangen, dass der Verantwortliche alle betroffenen Personen über die Beschaffung von Personendaten und bestimmte Rahmenbedingungen informiert. Weitere anwendbare Vorschriften in bestimmten Branchen können zusätzliche Informationspflichten auslösen. Zudem bestehen Einwilligungserfordernisse, insbesondere nach der DSGVO, u.U. aber auch nach dem nDSG und in Verbindung mit Geheimnisschutzvorschriften, wenn Bekanntgaben geplant sind.

17 *Erhebung bestehender Datenschutzerklärungen und Bearbeitungen*

Als Ausgangspunkt ist ein Verständnis der Bearbeitungsarten und der bestehenden Datenschutzinformationen erforderlich. Das verlangt zum einen die Erhebung von Bearbeitungen mit besonderen Informationspflichten (ggf. Profiling/Profiling mit hohem Risiko/automatisierte Einzelentscheidungen), zum anderen die Erhebung aller/der relevanten bestehenden DSE und -hinweise (auch z.B. in AGB).

Bei abgeschlossener DSGVO-Umsetzung: Prüfung der Aktualität der erhobenen Hinweise

Entsprechende Erhebungen sind auch nach dem nDSG notwendig.

18 *Prüfung der Anforderungen*

Zu prüfen ist weiter, wo Personendaten **gezielt beschafft** werden bzw. wo der Verantwortliche die Erhebung aktiv veranlasst – diese Vorgänge lösen Informationspflichten aus.

In Bezug auf **Einwilligungen** ist – je nach anwendbarem Recht –zu prüfen, ob ein Einwilligungserfordernis besteht oder eine

Bei abgeschlossener DSGVO-Umsetzung: Erhebung der bewussten Beschaffung bei betroffenen Personen in der Schweiz und der schweizerischen Gesellschaft(en) auch im Ausland

Auch das nDSG kennt eine generelle **Informationspflicht** bei der Beschaffung von Personendaten. Die Verletzung ist strafbedroht. Ebenfalls kennt das nDSG ein allgemeines

Information genügt und ob darüber hinaus spezialgesetzliche Informationspflichten und Einwilligungserfordernisse hinzukommen.

Ferner können, bei Geheimnissen, Entbindungserklärungen anfallen sowie zusätzliche Einwilligungen, wenn es um die Bekanntgabe besonders schützenswerter Personendaten geht.

Datengeheimnis, das je nach Umständen zu einem Einwilligungs- bzw. Befreiungserfordernis führen kann.

19 *Entwurf von DSE*

4 Erstmassnahme

Zu entscheiden ist zunächst über das Vorgehen, besonders dann, wenn mehrere ergänzende oder überschneidende Informationen in Frage kommen. Namentlich stellt sich die Ausgangsfrage, ob man **gruppenweite Standard-DSE** mit punktuellen Ergänzungen oder Abweichungen erstellen möchte oder individuelle DSE bevorzugt. Gestützt darauf sind die DSE zu entwerfen oder bestehende anzupassen. Je nach dem sind auch besondere Hinweise bei Schnittstellen mit Nutzern erforderlich, etwa beim Online-Handel, bei Kontaktformularen oder Chatbots. Nicht nur die DSE, auch die übrigen Dokumente wie Anträge, Informationsschreiben und AGB sollten laufend à jour gehalten werden.

Ein **Muster** für eine DSE nach der DSGVO und dem nDSG ist u.a. unter www.dsat.ch verfügbar.

Bei abgeschlossener DSGVO-Umsetzung: Entwurf ergänzender und/oder Anpassung bestehender DSE (Anpassungsbedarf i.d.R. beschränkt); Prüfung des Anpassungsbedarfs von AGB bzw. Vertragsunterlagen

Die gleichen Fragen stellen sich auch nach dem nDSG. Dabei sind aber **Besonderheiten zu beachten**. Immerhin verlangt das nDSG keinen expliziten Hinweis auf Profiling. Das gilt prinzipiell zwar auch bei einem hohen Risiko, doch ergibt sich hier i.d.R. eine Hinweispflicht aus dem Transparenzgrundsatz.

Anders als bei der DSGVO bestehen bei automatisierten Einzelentscheidungen Informationspflichten, aber keine Einwilligungserfordernisse. Eine Überbindung der Informationspflicht auf Dritte, wie z.B. einen Kunden, ist möglich.

Bestimmte Anforderungen gehen **über die DSGVO hinaus** (z.B. sind einzelne Empfängerstaaten/-regionen anzugeben). Zudem sind weitere Anpassungen von DSE auf Basis der DSGVO oft sinnvoll, etwa wenn es um Hinweise auf das anwendbare Recht, die Rechtsgrundlagen oder um Betroffenenrechte geht.

20 *Umsetzungsplanung*

Bei der Umsetzung bzw. dem **Roll-Out** neuer DSE stellen sich einige prozessuale Fragen, so z.B. die Abgrenzung zwischen Bestandes- und Neukunden bzw. passiver und aktiver Datenbearbeitung. Verweisungen auf eine DSE im Internet sind i.d.R. zulässig. Das gilt auch bei einer Drucksache. Allenfalls sind hier aber bestimmte Mindestinformationen im verweisenden Dokument anzubringen.

Beim Roll-Out stellen sich weitere Fragen der Umsetzung – in Frage kommen z.B. Hinweise beim Versand von Bestellbestätigungen oder Rechnungsbeilagen oder in E-Mail-Signaturen, aber auch eine Überbindung von Informationspflichten betr. Dritte auf einen Kunden in AGB. Schliesslich ist insbesondere bei Zweckänderungen an die Nachinformation zu denken.

Bei abgeschlossener DSGVO-Umsetzung: Planung der Bereitstellung revidierter bzw. neuer DSE und ggf. AGB

Analoge Fragen stellen sich auch nach dem nDSG. Im Besonderen ist im Rahmen des **Übergangsrechts** zu beachten, dass die Informationspflicht bei Bearbeitungen mit neuen «Beschaffungen» nach dem Inkrafttreten gilt – das kann auch auf Bestandeskunden Anwendung finden.

Datensicherheit

Die Datensicherheit ist ein Kernpunkt, der in der DSGVO und im nDSG inhaltlich aber wenig detailliert geregelt ist. Die Hauptvorgabe besteht darin, Sicherheitsrisiken zu erkennen und zu beurteilen und mit ihnen bewusst und verantwortungsvoll umzugehen. Inhaltliche Anforderungen ergeben sich vor allem aus anerkannten Standards, der Branchenüblichkeit, ggf. aus besonderen Vorschriften in einzelnen Branchen und Tätigkeiten und aus den Erwartungen von Kunden und Partnern.

21 *Datensicherheit*

5 Erstmassnahme

Die Datensicherheit ist aus rechtlicher, aber auch aus Reputationssicht, entscheidend. Die DSGVO enthält hier nur am Rande konkrete inhaltliche Vorgaben. Dennoch empfiehlt es sich, bestehende Applikationen und Prozesse auf Sicherheits- und verwandte Aspekte wie Privacy by Design oder Privacy by Default hin zu untersuchen, die Vollständigkeit der entsprechenden Dokumentation zu prüfen und in den Bearbeitungsverzeichnissen auf Sicherheitsmassnahmen hinzuweisen.

Bei abgeschlossener DSGVO-Umsetzung: Prüfung auf abweichende/besondere regulatorische bzw. sektorrechtliche Vorgaben

Inhaltlich ergeben sich kaum Abweichungen zwischen der DSGVO und dem nDSG, mit Ausnahme der Protokollierungsvorschriften nach der DSV (s. unten).

22 *Protokollierung*

Die DSV verlangt, dass Verantwortliche und Auftragsbearbeiter bestimmte Vorgänge wie das Verändern, Lesen, Bekanntgeben und Löschen von Personendaten protokollieren, soweit besonders schützenswerte Personendaten in grossem Umfang automatisiert bearbeitet oder ein Profiling mit hohem Risiko durchgeführt werden. Davon können eingeschränkte Ausnahmen bestehen. Die Protokolle müssen mindestens einem Jahr getrennt vom System aufbewahrt werden, in dem die Daten bearbeitet werden. Zudem dürfen Protokolle nur Organen und Personen zugänglich sein, die für den Datenschutz zuständig sind, und sie dürfen auch nur für diese Zwecke verwendet werden.

Es ist zu prüfen, ob die Voraussetzungen für die Pflicht zur Protokollierung gegeben sind. In diesem Fall muss geprüft werden, ob die entsprechenden Systeme in der Lage sind, die erforderlichen Protokollierungen durchzuführen und die Protokolle getrennt vom operativen System zu speichern.

Bei Verletzung droht möglicherweise ein Strafbarkeitsrisiko.

23 *Datenschutz-Folgenabschätzungen*

DSFA sind strukturierte Abklärungen von Risiken sowie des Umgangs mit diesen Risiken. Bei Bearbeitungen mit erhöhten Risiken können sie verpflichtend sein und eine Meldepflicht an Behörden auslösen.

Bei abgeschlossener DSGVO-Umsetzung: Prüfung auf abweichende/besondere regulatorische Vorgaben

Inhaltlich enthält das nDSG wenige Vorgaben und **kaum Abweichungen** von den Anforderungen der DSGVO. Eine Wiederholung von DSFA nach der DSGVO ist i.d.R. nicht

Bei ihrer Planung sind in erster Linie die **typischen Bearbeitungen** der Unternehmen zu bestimmen, die eine DSFA verlangen können, sowie allfällige **Ausnahmen** von der Durchführungspflicht. Mit Blick auf das Übergangsrecht ist sodann eine **zeitliche Abgrenzung** bei laufenden Bearbeitungen vorzunehmen.

Um den entsprechenden Prozess vorzubereiten, muss man sich über den **Auslöser** der DSFA verständigen, z.B. eine Information im Bearbeitungsverzeichnis, ferner die Rollen und Verantwortlichkeiten, den Einzug von DPO, IT und Business sowie den Abschluss und – bei hohen Restrisiken – die Meldung an Behörden. Hinsichtlich der Vorlagen kann es ggf. sinnvoll sein, unterschiedliche Muster für einfache und komplexe Fälle oder Mindest- und optionale Inhalte anzulegen. Schliesslich ist auf eine sorgfältige Dokumentation zu achten.

erforderlich. Eine Ausnahme der Pflicht zur Durchführung einer DSFA gilt bei einer gesetzlichen Pflicht zur entsprechenden Bearbeitung (z.B. im KYC-Bereich).

Ebenso besteht bei hohen Restrisiken analog zur DSGVO eine Meldepflicht gegenüber dem EDÖB, dies aber nur, wenn kein unabhängiger Datenschutzberater bestellt ist (vgl. Ziff. 6).

Eine Pflicht zur Durchführung von DSFA kennt das nDSG insbesondere bei einem «**Profiling mit hohem Risiko**», bei der umfangreichen Bearbeitung besonders schützenswerter Personendaten und bei der systematischen Überwachung umfangreicher öffentlicher Bereiche. Daneben ist eine freiwillige DSFA – wie auch nach der DSGVO – oft sinnvoll (wobei die Freiwilligkeit zu dokumentieren ist).

Nach der DSV sind DSFA für mindestens zwei Jahre nach Beendigung der entsprechenden Datenbearbeitung aufzubewahren.

24 *Datensicherheitsverletzungen*

Ein wesentlicher Punkt, den die DSGVO aber nicht sehr detailliert regelt, ist der Umgang mit Datensicherheitsverletzungen. Es besteht aber eine Pflicht zum angemessenen Umgang und u.U. zu einer Meldung an Behörden und Mitteilung an die betroffenen Personen. Es ist daher empfehlenswert, ein **Verfahren zum Umgang mit Verletzungen** (und ggf. weiteren «Incidents») einzurichten oder anzupassen. Hier ist insbesondere an eine Mitteilungspflicht der Mitarbeiter zu denken, aber auch an eine Regelung der Zuständigkeiten, Verantwortlichkeiten, Kontaktpunkte und einer geordneten Eskalation, ferner einer Meldepflicht gegenüber Behörden und betroffenen Personen. Die Verletzungen sind zu dokumentieren (vgl. Ziff. 9).

Auch nach dem nDSG muss mit Verletzungen kontrolliert umgegangen werden, und es kann eine **Meldepflicht** gegenüber dem EDÖB bestehen (aber mit einer höheren Schwelle als nach der DSGVO) und u.U. auch gegenüber den betroffenen Personen. Eine freiwillige Meldung beim EDÖB ist möglich, i.d.R. aber nicht empfohlen.

Drittparteien

Bei der Zusammenarbeit mit Drittparteien – d.h. vor allem mit Lieferanten, Kunden und Partnern – ergeben sich Vorgaben v.a. aus den Rollen der beteiligten Parteien. Die DSGVO und das nDSG definieren bestimmte Rollen und knüpfen bestimmte Rechtsfolgen an diese Rollen. Auch Datensicherheitsaspekte sind hier besonders relevant, und Datenbekanntgaben an Dritte sind in Bearbeitungsverzeichnissen zu erfassen und in DSE wiederzugeben.

25 *Bestehende Verträge*

Ausgangspunkt ist die **Prüfung bestehender Verträge** insbesondere mit Lieferanten und Kunden und die Bestimmung der entsprechenden Rollen (Verantwortlicher, gemeinsam Verantwortlicher, Auftragsverarbeiter).

Bei abgeschlossener DSGVO-Umsetzung: ggf. Prüfung weiterer Verträge für die Schweiz

26 *Lieferanten*

Bei Lieferanten stellt sich v.a. die Frage, ob/wann sie als Auftragsbearbeiter tätig sind und ob/wie sie eine angemessene Datensicherheit gewährleisten. Um die Lieferanten gehörig einzubinden, sind ggf. Anpassungen und Ergänzungen von **Verträgen** erforderlich, z.B. bei Auftragsbearbeitungen ohne entsprechende Regelungen.

Bei heikleren Bearbeitungen ist eine Prüfung der Lieferanten mit Zugang zu Personendaten («**Vendor Assessment**») zu definieren, während bei bestehenden Lieferanten u.U. ein Vendor (Re-)Assessment durchzuführen ist.

Ein **Standard-ADV** im Verhältnis zu Lieferanten (d.h. als Verantwortlicher) ist meistens notwendig. Unter Umständen ist es sinnvoll, Lieferantenverträge oder Vertragsklauseln zwischen unabhängig Verantwortlichen zu entwerfen.

Weitere Interaktionen mit Lieferanten aus datenschutzrechtlicher Sicht sind zu planen, wenn der Lieferant ein Verantwortlicher ist (z.B. Mitteilungen von Löschungen, Berichtigungen und Einschränkungen der Verarbeitung). Empfänger bzw. Kategorien von Empfängern sind im Bearbeitungsverzeichnis und in der DSE zu nennen.

Bei abgeschlossener DSGVO-Umsetzung: Prüfung und ggf. Anpassung von Lieferantenverträgen nach den gleichen Standards

Inhaltlich verlangt das nDSG für ADVs nicht mehr als die DSGVO (wobei für regulierte Unternehmen zusätzliche Anforderungen gelten können, z.B. für Banken und Versicherer). Es sind die **gleichen Massnahmen** wie nach der DSGVO erforderlich. Dabei bestehen Strafrisiken des Verantwortlichen bei fehlenden oder unzureichenden ADVs.

Soweit Lieferanten Zugang zu Personendaten haben, aber nicht als Auftragsbearbeiter tätig sind, ist eine Befreiung von Daten-/Berufsgeheimnissen zu prüfen. Soweit beide als gemeinsam Verantwortliche zusammenarbeiten, stellt das nDSG ebenfalls nicht höhere Anforderungen auf als die DSGVO.

Empfänger bzw. Kategorien von Empfängern sind im Bearbeitungsverzeichnis und in der DSE zu nennen.

27 *Kunden*

6 Erstmassnahme

Kundenseitig fragt sich v.a., wann das Unternehmen als **Auftragsbearbeiter** des Kunden tätig wird. Wichtig ist hier zudem – besonders wenn das Unternehmen IT-Leistungen erbringt – eine Dokumentation der angemessenen Datensicherheit. So wird das Unternehmen oft einen Standard-ADV in seiner Tätigkeit als Auftragsverarbeiter benötigen.

Bei abgeschlossener DSGVO-Umsetzung: Prüfung und ggf. Anpassung von Kundenverträgen nach den gleichen Standards

Wie erwähnt verlangt das nDSG nicht mehr für ADVs als die DSGVO. Auch die Anforderungen an Vereinbarungen zwischen gemeinsam Verantwortlichen sind nicht höher, sogar im Gegenteil. Im Übrigen sind Empfänger bzw. Kategorien von Empfängern im Bearbeitungsverzeichnis und in der DSE zu nennen.

Unter Umständen ist ausserdem eine Standard-Vereinbarung zwischen gemeinsam Verantwortlichen sinnvoll, doch kann sie meist auch ad hoc geschlossen werden. Auch Standard-Vertragsbestimmungen mit anderen unabhängig Verantwortlichen können sinnvoll sein.

Weitere Interaktionen mit Kunden aus datenschutzrechtlicher Sicht sind zu planen, wenn das Unternehmen ein Verantwortlicher ist (z.B. Mitteilungen von Löschungen, Berichtigungen und Einschränkungen der Verarbeitung).

28 *Grenzüberschreitende Übermittlungen*

Die Übermittlung von Personendaten ist nach der DSGVO beschränkt, d.h. unter Umständen nur mit besonderen Schutzmassnahmen, erlaubt. Diese Beschränkungen betreffen etwa Bekanntgaben in die USA, nach Indien und in andere Staaten ausserhalb des EWR (sog. «Drittstaaten»).

Zu erheben sind bestehende **grenzüberschreitende Übermittlungen** innerhalb (vgl. Ziff. 29) und ausserhalb des Konzerns. Dabei gilt es jeweils die Angemessenheit des Schutzniveaus im Empfängerstaat zu prüfen (d.h. ob das Schutzniveau von der EU-Kommission als angemessen anerkannt wurde). Des Weiteren sind bei Übermittlungen in Drittstaaten **Datenübermittlungsverträge** zu prüfen (z.B. die Standardvertragsklauseln der EU). Die Europäische Kommission hat am 12. November 2020 revidierte Standardklauseln im Entwurf veröffentlicht. Bevor diese in Kraft treten, sind Verträge, welche die Klauseln enthalten, anzupassen.

Bei abgeschlossener DSGVO-Umsetzung: Anpassung von Standardvertragsklauseln an die Schweiz i.d.R. nicht zwingend, aber u.U. Meldung an den EDÖB erforderlich

Inhaltlich decken sich die Anforderungen des nDSG mit jenen der DSGVO. Es bestehen namentlich **Strafrechtsrisiken** bei unzulässiger Auslandsübermittlung. Zusätzlich zu beachten sind Geheimnisschutzvorschriften, bspw. nach Art. 273 StGB und nach sektorrechtlichen Vorgaben.

Seit der Europäische Gerichtshof (EuGH) im «**Schrems II**»-Urteil den Privacy Shield aufgehoben hat und bei Verwendung der Standardvertragsklauseln eine Risikoeinschätzung verlangt, können weitere Massnahmen erforderlich sein. Dazu gehören ggf. die Prüfung bestehender Verträge mit Empfängern in Drittstaaten, die Durchführung einer Beurteilung der sich aus der Bekanntgabe ergebenden besonderen Risiken («**Transfer Impact Assessment**», «TIAs»), ggf. ein Wechsel des Privacy Shield auf Standardklauseln und u.U. auch eine Ergänzung der Standardklauseln. Soweit

Inhaltlich verlangt das nDSG auch hier nicht mehr als die DSGVO. Der EDÖB verlangt aber ebenfalls eine Risikobeurteilung und ggf. eine Ergänzung der Standardvertragsklauseln.

Bearbeitungsverzeichnisse und DSE auf den Privacy Shield Bezug nehmen, sind auch hier Anpassungen nötig.

Konzerninterne Datenflüsse

Im Grundsatz gelten im Datenverkehr innerhalb eines Konzerns die gleichen Regeln wie bei der Zusammenarbeit mit Dritten und grenzüberschreitenden Datenübermittlungen an Aussenstehende. Meist werden hier aber besondere, auf das Konzernverhältnis angepasste Regelungen getroffen.

29 *Regelung konzerninterner Datenflüsse (Rollen und grenzüberschreitende Übermittlungen)*

Konzerninterne Datenflüsse werden i.d.R. besonders geregelt, auf **Einzelfallbasis** oder in Form einer **Rahmenvereinbarung**. Nebst der Erhebung konzerninterner Datenflüsse ist hier an die Prüfung und ggf. den Abschluss oder die Ergänzung eines Rahmenvertrags («IGDTA» bzw. «IDPA») zu denken, wobei die erfassten Datenflüsse und -bearbeitungen i.d.R. zentral erfasst werden müssen (vgl. Ziff. 9).

Alternativ können bestehende Verträge z.B. durch interne ADV, Vereinbarungen zwischen gemeinsam Verantwortlichen und/oder Standardvertragsklauseln bei grenzüberschreitenden Übermittlungen ergänzt werden. Auch konzerninterne Empfänger sind in Bearbeitungsverzeichnissen und DSE zu erfassen (bspw. als eine Kategorie von Empfängern).

Bei abgeschlossener DSGVO-Umsetzung: Prüfung bestehender konzerninterner Grundlagen; i.d.R. nur punktuelle Anpassungen erforderlich

Soweit ein Rahmenvertrag nach den Vorgaben der DSGVO besteht, sind i.d.R. nur wenige Anpassungen an das nDSG erforderlich. Bei unzulässiger Auslandsübermittlung bestehen **Strafrechtsrisiken**. Besonders zu prüfen sind u.U. ferner Daten-/Berufsgeheimnisvorschriften.

Auch nach dem nDSG sind konzerninterne Empfänger als eine Kategorie in Bearbeitungsverzeichnissen und DSE zu erfassen – anders als nach der DSGVO aber unter Angabe der Empfängerstaaten.

Betroffenenrechte

Betroffene Personen haben bestimmte Rechte (z.B. ein Auskunfts- und ein Berichtigungsrecht). Die Einhaltung der Betroffenenrechte ist rechtlich, aber auch aus Reputationsgründen, besonders wichtig.

30 *Umgang mit Betroffenenrechten*

Für den Umgang mit Betroffenenrechten bestehen relativ **detaillierte Vorgaben**. In einem ersten Schritt sind die entsprechenden Prozesse zu planen. Neben der Festlegung von Gegenstand und Umfang je nach Häufigkeit sind dabei insb. die Betroffenen zu identifizieren, interne Zuständigkeiten festzulegen, die Zulässigkeit der Rechte und deren Ausnahmen abzuklären, und zu bestimmen, wie die erforderlichen Informationen zu erheben, zusammenzustellen

Bei abgeschlossener DSGVO-Umsetzung: Anpassung bestehender Prozesse und Musterdokumente

Beim Gegenstand und dem Umgang mit Anfragen von Betroffenen bestehen teilweise deutliche **Abweichungen gegenüber der DSGVO** (z.B. betr. Ablauf und Ausnahmen). Bei bestimmten Verletzungen bestehen Strafrechtsrisiken.

und bei Auskunftsbegehren mitzuteilen sind. Die Hinweise in DSE sind mit diesen Prozessen abzugleichen, etwa betreffend Kommunikationskanäle, Identifikation und Zuständigkeiten. Schliesslich ist die technische Umsetzung zu bedenken und insbesondere die Fähigkeit zu Auskunft, Löschung (siehe Ziff. 30 f.) und Datenportabilität.

31 *Korrespondenz*

Bei häufigeren Anfragen ist zu prüfen, ob Musterkorrespondenz erstellt soll.

Bei abgeschlossener DSGVO-Umsetzung: Prüfung und ggf. Anpassung von Musterkorrespondenz

Bestimmte Abweichungen von der DSGVO ergeben sich auch bei der Reaktion auf Betroffenenanfragen.

Aufbewahrung und Löschung

Ein Kernpunkt bei der datenschutzrechtlichen Compliance ist die Löschung oder Anonymisierung von Personendaten, die nicht mehr benötigt werden (d.h. nachdem der Zweck der Bearbeitung erreicht wurde). Die kontrollierte Löschung nach bestimmten Ereignissen oder Fristen stellt in erster Linie Anforderungen an die IT.

32 *Löschfähigkeit*

Entscheidend ist die technische Fähigkeit zu definierter Aufbewahrung und gesteuerter Löschung; ggf. ist dies als eigenes Teilprojekt auszugestalten.

Inhaltlich verlangt das nDSG in diesem Bereich nicht mehr als die DSGVO.

33 *Löschkonzept*

Erforderlich ist – als Grundlage einer (teil-technischen) Lösung – eine Regelung der Aufbewahrungsfristen und -arten je nach Kategorie oder Klassifizierung von Daten und der Löschungen bzw. Anonymisierungen («Retention Policy»).

Bei abgeschlossener DSGVO-Umsetzung: Ergänzung bestehender Retention Policies; ggf. Planung systemseitiger Anpassungen

Schulungen

Weder die DSGVO noch das nDSG verlangen explizit Schulungen. Sie sind aber oft faktisch notwendig bzw. hilfreich, können haftungsreduzierend wirken und sind u.U. als Teil der Governance und der Accountability auch rechtlich zwingend.

34 *Gegenstand*

Schulungsmassnahmen sind insbesondere hinsichtlich ihrer Adressaten (z.B. alle Mitarbeiter, bestimmte Mitarbeiter, bestimmte Bereiche des Unternehmens usw.), ihres Inhalts, ihrer Häufigkeit und der Erfolgsmessung zu planen.

35 *Umsetzung*

Schulungsmaterial kann eingekauft oder vom Unternehmen selbst erstellt bzw. angepasst werden.

Bei abgeschlossener DSGVO-Umsetzung: ggf. Anpassung bestehenden Schulungsmaterials

Abkürzungen

ADV	Auftragsdatenverarbeitungsvereinbarung zwischen Verantwortlichem und Auftragsverarbeiter
DPO	Datenschutzbeauftragter (DPO, Data Protection Officer) i.S.d. DSGVO
DSE	Datenschutzerklärung(en)
DSFA	Datenschutz-Folgenabschätzung(en)
DSG	Datenschutzgesetz der Schweiz. Dazu gehört auch eine Verordnung (VDSG)
DSGVO	EU-Datenschutz-Grundverordnung (Verordnung (EU) 2016/679)
DSV	revidierte Verordnung zum nDSG (in Kraft am 1. September 2023)
EU	Europäische Union
EuGH	Gerichtshof der Europäischen Union
EWR	Europäischer Wirtschaftsraum (neben der EU auch Liechtenstein, Norwegen und Island)
nDSG	revidiertes DSG der Schweiz (in Kraft am 1. September 2023)

Walder Wyss AG
Rechtsanwälte

Telefon +41 44 498 98 98
reception@walderwyss.com

www.walderwyss.com
Zürich, Genf, Basel, Bern, Lausanne, Lugano

Kontakte

Jürg Schneider
Dr. iur., Rechtsanwalt
Partner
Telefon direkt: +41 58 658 55 71
juerg.schneider@walderwyss.com

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

Unser Datenschutz-Team

Bernadette Bucheli
MLaw, Rechtsanwältin, CIPP/E, CIPM
Associate
Telefon direkt: +41 58 658 58 23
bernadette.bucheli@walderwyss.com

Marco Galli
lic. oec. HSG, Rechtsanwalt
Managing Associate
Telefon direkt: +41 58 658 44 11
marco.galli@walderwyss.com

Caroline Gaul
LL.M., Rechtsanwältin (Rechtsanwaltskammer Frankfurt a.M.)
Senior Associate
Telefon direkt: +41 58 658 51 35
caroline.gaul@walderwyss.com

Lena Götzinger
Rechtsanwältin (Rechtsanwaltskammer Frankfurt a.M.)
Associate
Telefon direkt: +41 58 658 56 63
lena.goetzinger@walderwyss.com

Michael Isler
Dr. iur., Rechtsanwalt
Partner
Telefon direkt: +41 58 658 55 15
michael.isler@walderwyss.com

Oliver M. Kunz
lic. iur., LL.M., Rechtsanwalt
Partner
Telefon direkt: +41 58 658 56 41
oliver.kunz@walderwyss.com

Hugh Reeves
MLaw, LL.M., Rechtsanwalt
Senior Associate
Telefon direkt: +41 58 658 52 73
hugh.reeves@walderwyss.com

Mark A. Reutter
Dr. iur., LL.M., Rechtsanwalt
Partner
Telefon direkt: +41 58 658 55 42
mark.reutter@walderwyss.com

Florian C. Roth
MLaw, Rechtsanwalt
Associate
Telefon direkt: +41 58 658 55 79
florian.roth@walderwyss.com

Christine Schweikard
LL.M. (KCL), Maîtrise en droit (Paris II), Rechtsanwältin (Rechtsanwaltskammer München), Associate
Telefon direkt: +41 58 658 58 33
christine.schweikard@walderwyss.com

Monique Sturny
Dr. iur., LL.M., Rechtsanwältin
Managing Associate
Telefon direkt: +41 58 658 56 56
monique.sturny@walderwyss.com

Monja Sieber
MLaw, Rechtsanwältin
Associate
Telefon direkt: +41 58 658 29 16
monja.sieber@walderwyss.com

Martin Zobl
Dr. iur., LL.M., Rechtsanwalt
Managing Associate
Telefon direkt: +41 58 658 55 35
martin.zobl@walderwyss.com

Michael Schmassmann
M.A HSG in Law, Rechtsanwalt
Associate
Telefon direkt: +41 58 658 52 59
michael.schmassmann@walderwyss.com