Ihre Spende
in guten Händen.

UMSETZUNGSHILFE ZUM NEUEN DATENSCHUTZGESETZ

August 2023

Herausgeberin:
Stiftung Zewo

Autorinnen:
Bernadett Gal
Martina Ziegerer

Juristische Beratung:
Martin Steiger

Impressum und Kontakt
Stiftung Zewo
Pfingstweidstrasse 10
8005 Zürich
info@zewo.ch
zewo.ch
+41 44 366 99 55

Inhaltsübersicht

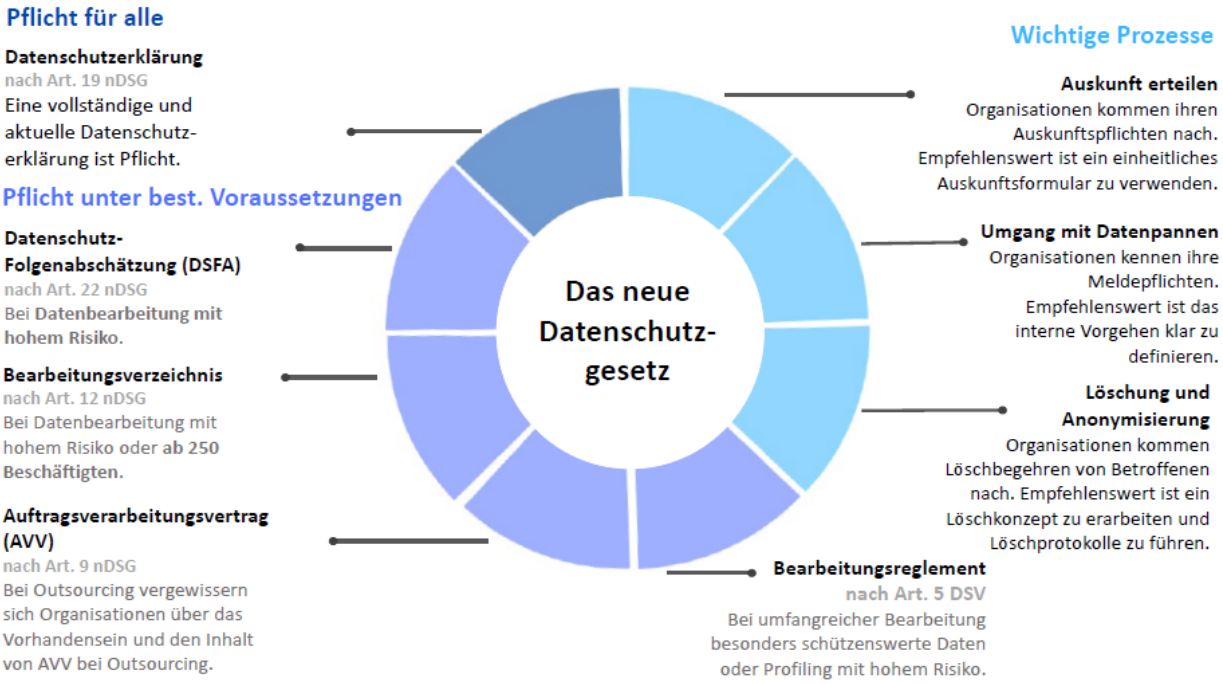
Datenschutz - so setzen NPO das neue Gesetz um

Was müssen Hilfswerke tun, um das neue Datenschutzgesetz einzuhalten? Diese Umsetzungshilfe der Stiftung Zewo informiert, wer welche Dokumente erstellen muss. NPO erhalten praktische Tipps, wie sie dabei am besten vorgehen und erfahren, was die Zewo in Bezug auf den Datenschutz künftig verlangt.

Das revidierte Gesetz schützt die Persönlichkeit und die Grundrechte von natürlichen Personen, deren Personendaten Ihre Organisation sammelt und bearbeitet. Das neue Datenschutzgesetz (nDSG) und die dazugehörige Verordnung gelten ab dem 1. September 2023 ohne Übergangsfrist.

Das revidierte Datenschutzgesetz finden Sie unter folgendem Link, die dazugehörige Verordnung (DSV) hier. Zudem hat das Bundesamt für Justiz (BJ) am 1. Februar 2023 nützliche Frequently Asked Questions (FAQ) zum revidierten Datenschutzgesetz herausgegeben. Diese FAQ finden Sie hier.

Mit dieser Umsetzungshilfe erkennen Hilfswerke schnell und einfach, wozu sie konkret verpflichtet sind und welche Vorkehrungen sie treffen sollen. Sie folgt den unten aufgeführten Dokumenten und Prozessen, die das neue Gesetz regelt.



Was die Zewo von zertifizierten NPO verlangt

Der Zewo-Standard 19 «Datenschutz» wird zurzeit überarbeitet und voraussichtlich per 1.1.2024 an die Gesetzesänderung angepasst. Die Genehmigung durch den Zewo-Stiftungsrat und allfällige Anpassungen bleiben vorbehalten.

Die neuen Bestimmungen im Standard gehen nicht über die gesetzlichen Anforderungen hinaus. Vielmehr greift der Standard auf, welche gesetzlichen Bestimmungen im Hinblick auf Spendende

besonders wichtig sind. Bei der Erst- und Rezertifizierung prüft die Zewo, ob die Organisation den Standard 19 einhält. Vorgaben des Standards, welche bereits heute über die gesetzlichen Mindestanforderungen hinausgehen, bleiben bestehen.

Diese Grundsätze werden im Zewo-Standard 19 verankert

Die Organisation respektiert den Datenschutz und die Privatsphäre von betroffenen natürlichen Personen, insbesondere der Spenderinnen und Spender.
Zewo-Standard 19 Absatz 1, voraussichtlich ab 01.01.2024 in Kraft

Die Organisationen halten sich an das anwendbare und aktuelle Datenschutzgesetz. Insbesondere kennen sie ihre Informations- sowie Dokumentationspflichten und wahren die Rechte der betroffenen Personen. Die Sammlung von Personendaten erfolgt nur, wenn diese für die Zwecke der Organisation notwendig sind, sparsam im dafür nötigen Ausmass.
Zewo-Standard 19 Absatz 2, voraussichtlich ab 01.01.2024 in Kraft

Das ist wichtig für den Datenschutz

Das neue Gesetz soll ein einheitliches Verständnis davon schaffen, was derzeit für den Datenschutz generell wichtig ist. Es will Organisationen sowie deren Mitarbeitende und Partner sensibilisieren, transparent zu handeln, auf die Persönlichkeitsrechte von natürlichen Personen zu achten, diese zu wahren und die Daten zu sichern. Organisationen sollen Prozesse, Systeme, Strukturen und Verträge identifizieren, analysieren und nötigenfalls optimieren, mit denen sie Daten von natürlichen Personen erheben, verwalten oder anderweitig bearbeiten. Dabei soll der organisatorische Aufwand im Bereich des Datenschutzes auf die Grösse und Strukturen der jeweiligen Organisationen, sowie auf die Art und Menge der Datenbearbeitung angepasst sein. Bezüglich des Umsetzungsbedarfs von Organisationen gibt es erhebliche Unterschiede.

Um das revidierte Datenschutzgesetz umzusetzen, sollten Hilfswerke dem Datenschutz die nötige Aufmerksamkeit schenken. Das bedeutet: die benötigten Kapazitäten bereitstellen und intern Verständnis für das Thema schaffen.

Eine aktuelle Datenschutzerklärung - ein Muss für alle

Gesetzliche Norm Art. 19 ff nDSG

Eine aktuelle Datenschutzerklärung ist für alle Organisationen unerlässlich, denn sie stellt einen Teil ihrer Informationspflicht dar. Eine Datenschutzerklärung trägt zu einer transparenteren

Datenbearbeitung bei und ermöglicht betroffenen Personen, ihre Rechte auszuüben. Mittels Datenschutzerklärung deklarieren Sie, welche Daten Sie von natürlichen Personen wozu beschaffen. Überprüfen Sie also Ihre bestehende Datenschutzerklärung und aktualisieren Sie diese, wo nötig. Bereits vor der Revision des Datenschutzgesetzes verlangte Standard19 eine klare, gut sichtbare, einfach aufrufbare und aktuelle Datenschutzerklärung.

Diese Inhalte gehören in die Datenschutzerklärung

Die Datenschutzerklärung informiert darüber, wer welche Daten sammelt und weshalb. Sie hält fest, über welche Personen Ihre Organisation Daten sammelt und wie sie diese bearbeitet. Das Gesetz verlangt, dass Datenschutzerklärungen mindesten das Folgende beinhalten:

- Identität und Kontaktdaten der verantwortlichen Organisation
- Zwecke, für welche Ihre Organisation die Daten sammelt und bearbeitet
- allfällige Empfängerinnen und Empfänger der gesammelten Daten
- allfälliger Daten-Export ins Ausland
- allfällige automatisierte Einzelentscheidungen

Weitere mögliche Angaben sind Informationen über:

- die Kategorien der gesammelten Personendaten
- den Kreis der betroffenen Personen
- die Rechte der betroffenen Personen und wo diese geltend gemacht werden können
- die Verwendung von Cookies, Tracking und anderen Technologien
- das Vorgehen der Organisation zur Gewährleistung der Datensicherheit

Das verlangt die Zewo bezüglich Datenschutzerklärung

Spenden sammelnde Organisationen verfügen über eine klare, gut sichtbare, einfach aufrufbare und aktuelle Datenschutzerklärung auf ihrer Webseite. Die Datenschutzerklärung entspricht den gesetzlichen Vorgaben. Sie informiert insbesondere darüber, welche Personendaten zu welchen Zwecken beschafft und bearbeitet werden.

Zudem nennt die Datenschutzerklärung den Namen der Spenden sammelnden Organisation sowie eine Kontaktadresse, an die sich betroffene Personen für datenschutzrechtliche Belange wenden können. Die Datenschutzerklärung regelt ausserdem die allfällige Bekanntgabe von personenbezogenen Daten ins Ausland und die Rechte der Betroffenen.

Zewo-Standard 19 Absatz 5, voraussichtlich ab 01.01.2024 in Kraft

Tipps der Zewo

Platzieren Sie die Datenschutzerklärung leicht zugänglich auf Ihrer Webseite, idealerweise im Footer, und weisen Sie deutlich darauf hin. Aktualisieren Sie die Datenschutzerklärung Ihrer Organisation mindestens jährlich.

Hier erhalten Sie Unterstützung

- Eine Musterdatenschutzerklärung finden Sie über das Datenschutz Self Assessment Tool (DSAT) hier oder auf der Webseite von ProFonds hier.
- **Hinweis**: Juristische Berater, wie zum Beispiel die Datenschutzpartner AG, erstellen und aktualisieren Ihre Datenschutzerklärung mit dem kostenpflichtigen Datenschutz-Generator. Nutzen Sie den Rabatt, welchen die Datenschutzpartner AG Zewo-zertifizierten Hilfswerken gewährt. Ihren Zewo-Rabatt finden Sie unter folgendem Link.

Datenschutz-Folgenabschätzung (DSFA)

Gesetzliche Norm Art. 22 nDSG

Wer braucht eine Datenschutz-Folgenabschätzung?

Organisationen, deren geplante Bearbeitung von personenbezogenen Daten potenziell ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringen kann.

Was ist eine Datenschutz-Folgenabschätzung?

Die Datenschutz-Folgenabschätzung ist ein Risikomanagement-Instrument, welches angewendet wird, um festzustellen, ob die geplante Bearbeitung von personenbezogenen Daten ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen natürlichen Personen birgt. Sie ist vor einer geplanten Datenbearbeitung, als Risikoprävention, auszuarbeiten.

Ein **hohes Risiko** kann sich aus der Art, dem Umfang, den Umständen, dem Zweck der Datenbearbeitung sowie durch die Verwendung neuer Technologien ergeben. Ein mit der Datenbearbeitung verbundenes hohes Risiko besteht grösstenteils, wenn besonders schützenswerte Personendaten bearbeitet werden.

Um **besonders schützenswerte Personendaten** handelt es sich bei Informationen über die Aspekte der Persönlichkeit von natürlichen Personen, wie beispielsweise Angaben zur religiösen oder weltanschaulichen Überzeugung, sexuellen Orientierung, politischen Meinung oder auch **Gesundheitsdaten.**

➔ ***Ein Praxisbeispiel:*** *Ein Heim für Menschen mit Beeinträchtigungen, welches seinen Bewohnenden Medikamente abgibt oder andere medizinische Behandlungen durchführt, benötigt, bearbeitet und speichert dafür die Krankengeschichte beziehungsweise Gesundheitsdaten der Bewohnenden. In diesem Fall bearbeitet die Organisation Personendaten mit hohem Risiko, denn Gesundheitsdaten sind besonders schützenswerte Personendaten.*

Worum geht es bei einer Datenschutz-Folgenabschätzung?

Die potenziell hohen Risiken ihrer Datenbearbeitung müssen Organisationen immer im Einzelfall beurteilen. Dies tun sie im Rahmen ihrer Datenschutz-Folgenabschätzungen. Mittels Datenschutz-Folgenabschätzung erkennen Organisationen bereits vorgängig, welche potenziell hohen Risiken für Betroffene ihre geplante Datenbearbeitung beinhalten kann. Organisationen definieren und überprüfen geeignete Massnahmen für die Gewährleistung der Datensicherheit von Personendaten.

Erkennen Organisationen durch ihre Datenschutz-Folgenabschätzungen trotz definierter Gegenmassnahmen Risiken, welche zu unerwünschten negativen Folgen ihrer Datenbearbeitung führen könnten, nehmen sie fachliche Unterstützung in Anspruch.

Das verlangt die Zewo bezüglich Datenschutzfolgen-Abschätzung

Es kommen die einleitend im **Zewo-Standard 19 Absatz 2** festgehaltenen Grundsätze zur Anwendung. Die Anforderungen der Zewo gehen nicht über die gesetzlichen Rahmenbedingungen hinaus. Eine Datenschutz-Folgenabschätzung verlangt die Zewo lediglich von Organisationen, welche hierzu gesetzlich verpflichtet sind.

Mittels Datenschutz-Folgenabschätzung erkennen Organisationen die potenziell hohen Risiken ihrer beabsichtigten Datenbearbeitung, bewerten diese und definieren Massnahmen, um potenzielle Datenschutzverletzungen zu vermeiden, sollte ihre geplante Bearbeitung hohe Risiken bergen.

Tipps der Zewo

Die Zewo rät den zertifizierten Organisationen, welche gesetzlich verpflichtet sind eine Datenschutz-Folgenabschätzung zu erstellen, risikogerecht und mit angemessenem Aufwand einen Prozess für die Erstellung von Datenschutz-Folgenabschätzungen zu etablieren, diese zu verschriftlichen und die personellen Zuständigkeiten zu regeln. Es ist ausserdem ratsam, in einer Datenschutz-Folgenabschätzung die folgenden Punkte zu berücksichtigen:

- Beschreibung der geplanten Datenbearbeitung
- Erstellung einer Risikoanalyse
- Identifikation von besonderen Risikofaktoren
- Risikobewertung nach Schwere und Eintrittswahrscheinlichkeit
- mögliche Massnahmen im Umgang mit potenziellen Risiken

Hier erhalten Sie Unterstützung

Eine mögliche Hilfestellung für die Ausarbeitung einer Datenschutz-Folgenabschätzung bieten beispielsweise die Grundlagendokumente «Merkblatt Datenschutz-Folgenabschätzung DSFA» und «Formular Datenschutz-Folgenabschätzung (DSFA)» der Datenschutzbeauftragten des Kantons Zürichs. Diese Dokumente sind unter diesem Link auffindbar. Die inhaltlichen Angaben bieten eine hilfreiche Orientierung für die Ausgestaltung einer DSFA.

Führung eines Verarbeitungsverzeichnisses

Gesetzliche Norm Art. 12 nDSG

Wer braucht ein Inventar über die verarbeiteten Personendaten?

Organisationen, welche 250 oder mehr Beschäftigte haben und/oder Organisationen, deren Datenbearbeitung hohe Risiken für Betroffene bergen.

Was ist ein Verarbeitungsverzeichnis?

Organisationen sowie auch ihre Auftragsbearbeiter werden von Gesetzes wegen verpflichtet, ein Verzeichnis über ihre Bearbeitungstätigkeiten zu führen. Das Verarbeitungsverzeichnis sollte keine konkrete Auflistung einzelner Datenbearbeitungen sein, sondern eine generelle Beschreibung der Bearbeitungstätigkeit einer Organisation. Ein solches Verzeichnis wird auch Daten-Inventar genannt. Von der Führung eines Verzeichnisses sind Organisationen **befreit**, wenn sie weniger als 250 Mitarbeitende beschäftigen sowie keine Bearbeitung von besonders schützenswerten Personendaten in grossem Umfang erfolgt und kein Profiling mit hohem Risiko durchgeführt wird.

Wozu das Inventar dient: Dank des Daten-Inventars gewinnen Sie einen Überblick, wo innerhalb Ihrer Organisation Daten von natürlichen Personen gesammelt, bearbeitet oder gespeichert werden. Die wichtigsten Fälle können Sie durchspielen, optimieren und dokumentieren.
Was das Inventar beinhaltet: Es erfasst die Bereiche, Prozesse und Kontexte in Ihrer Organisation, in denen Daten von natürlichen Personen erhoben, bearbeitet oder gesammelt werden.
Darauf sollten Sie beim Erstellen des Inventars achten: Es ist ratsam, ein normiertes und systematisches Inventar zu erstellen. Dokumentieren und begründen Sie den Datenbesitz und die Datenbearbeitung.

Denken Sie dabei an unterschiedliche Personenkreise wie etwa: Mitarbeitende, Auftragnehmende, Empfängerinnen und Empfänger von Leistungen, mögliche, aktuelle oder ehemalige Spenderinnen und Spender, Freiwillige oder Sympathisierende.

Bezeichnen Sie die Verantwortlichen für den jeweiligen Bereich oder Prozess.

Hier erhalten Sie Unterstützung

Eine Hilfestellung finden Sie hier auf der Website von Datenschutz Self Assessment Tool DSAT. Das Dokument «Inventar – Überblick der Datenbearbeitungen» bietet eine nützliche Vorlage.

Das verlangt die Zewo bezüglich Verarbeitungsverzeichnis

Es kommen die einleitend im **Zewo-Standard 19 Absatz 2** festgehaltenen Grundsätze zur Anwendung. Die Anforderungen der Zewo gehen nicht über die gesetzlichen Rahmenbedingungen hinaus. Ein Verarbeitungsverzeichnis verlangt die Zewo lediglich von Organisationen, welche hierzu gesetzlich verpflichtet sind.

Tipps der Zewo

Die Zewo rät auch anderen zertifizierten Organisationen, sich auf freiwilliger Basis und mit angemessenem Aufwand mit dem Thema zu befassen, um sich einen Überblick über die in der Organisation bearbeitet Daten zu verschaffen. Denn ohne Daten-Inventar ist es kaum möglich, das Datenschutzrecht einzuhalten. DSAT stellt hier ein vorgefertigtes Formular benannt als «Inventar – Datenbearbeitung (für Verantwortliche)» zur Verfügung.

Vertrag über die Auftragsverarbeitung (AVV)

Gesetzliche Norm Art. 9 nDSG

Die Bearbeitung von Personendaten kann gemäss Gesetz (Art. 9 nDSG) an Auftragsbearbeitende übertragen werden. Auftragsverarbeitungsverhältnisse liegen beispielsweise vor bei: Hosting, Cloud-Sicherung, Apps wie zum Beispiel Microsoft 365, Finanz- und Lohnbuchhaltung, Hosting- und Data-Center-Dienstleistungen, Analysen und Datenanreicherung, Abgleich von Fremdadressen, Werbe- und Fundraising-Agenturen, Lettershops sowie bei Tracking auf verschiedenen digitalen Plattformen und Datenweiterverarbeitung.

Auch wenn die Datenverarbeitung an Dritte delegiert wird, verbleibt die Verantwortung für den Datenschutz bei der Organisation, die den Auftrag erteilt hat. Auftragsverarbeitungsverträge sichern das Outsourcing ab.

Das verlangt die Zewo bezüglich Auftragsverarbeitungsvertrag

Die Zewo verlangt von den zertifizierten Organisationen, welche mit Auftragsverarbeitenden zusammenarbeiten, dass sie ihre Verträge mit solchen Dritten überprüfen. Konkret bedeutet dies, dass Organisationen die sichere und adäquate Bearbeitung ihrer Daten durch Dritte gewährleisten. Sie tun dies vor allem, indem sie ihre Auftragsverarbeitenden sorgfältig auswählen und instruieren, einen geeigneten Auftragsverarbeitungsvertrag eingehen und die technischen und organisatorischen Massnahmen zur Gewährleistung der Datensicherheit des bearbeitenden Dritten überprüfen.
Zewo-Standard 19 Absatz 7, voraussichtlich ab 01.01.2024 in Kraft

Hinweis: In diesem Kontext muss darauf geachtet werden, ob im Rahmen der Bearbeitung durch Dritte eine Datenübermittlung ins Ausland stattfindet. Eine Liste der Staaten im Ausland, deren Recht einen angemessenen Datenschutz gewährleistet, wird in Anhang 1 der Datenschutzverordnung, DSV geführt. Diese Liste wird periodisch überprüft und angepasst. Organisationen, welche ihre Datenbearbeitung an Dritte mit Sitz im Ausland auslagern, sollten diese Liste regelmässig konsultieren.

Tipps der Zewo

Die Zewo rät zertifizierten Organisationen, ihre Verträge mit Subunternehmern systematisch zu analysieren, um zu prüfen, ob die Sicherheit der Daten technisch und inhaltlich gewährleistet werden kann. Adäquate technische und organisatorische Massnahmen für die Wahrung der Datensicherheit werden in Art. 3 DSV genauer umschrieben. Schliesslich rät die Zewo den Organisationen, ihre Auftragsverarbeitenden sorgfältig auszuwählen und zu instruieren.

Bearbeitungsreglement

Gesetzliche Norm Art. 5 DSV (Verordnung über den Datenschutz)

Wer muss ein Bearbeitungsreglement erstellen?

Organisationen, welche entweder umfangreich besonders schützenswerte Personendaten bearbeiten oder ein Profiling mit hohem Risiko durchführen.

Die Pflicht zur Erstellung eines Bearbeitungsreglements ist nicht im Gesetz, sondern auf Verordnungsebene verankert. Gemäss den Bestimmungen der Verordnung müssen Verantwortliche, somit auch Organisationen sowie ihre Auftragsbearbeiter, ein Reglement für automatisierte Bearbeitungen erstellen, wenn sie **Profiling mit hohem Risiko** erstellen oder in grossem Umfang **besonders schützenswerte Personendaten** bearbeiten. Das Bearbeitungsreglement soll als Handbuch für eine automatisierte Datenbearbeitung dienen und zur Förderung der Rechenschaftspflicht von Organisationen beitragen.

Was ist «Profiling» und «Profiling mit hohem Risiko»

Der Begriff «Profiling» umfasst jegliche Art der automatisierten Bearbeitung von personenbezogenen Daten, mit deren Hilfe gewisse persönliche Aspekte einer natürlichen Person analysiert werden können. Unter Aspekte der Persönlichkeit einer natürlichen Person fallen beispielsweise Angaben zu ihrer Gesundheit, persönliche Vorlieben und Interessen, wirtschaftliche Situation und Aufenthaltsorte. Mittels «Profiling» kann folglich eine Person eingeschätzt oder beurteilt werden. Eine solche Einschätzung kann sich auf bestehende Merkmale der Persönlichkeit einer Person beziehen oder als eine Voraussage für künftige Verhaltensweisen dienen. Ein «Profiling mit hohem Risiko» birgt ein hohes Risiko für die Persönlichkeit oder für die Grundrechte von betroffenen natürlichen Personen, indem die Bearbeitung der Daten zu einer Verknüpfung einer Vielzahl von Daten führt, welche die Beurteilung von **wesentlichen** Aspekten der Persönlichkeit ermöglicht. Wesentliche Aspekte der Persönlichkeit schliessen beispielsweise ausserberufliche Beziehungen oder Tätigkeiten, Weltanschauung oder das Konsumverhalten mit ein. Die praktische Relevanz der Bestimmung zum Profiling mit hohem Risiko wird sich noch zeigen.

Gesetzliche Mindestanforderungen

Artikel 5 DSV führt die gesetzlichen Mindestanforderungen an das Bearbeitungsreglement aus. Die Mindestanforderungen umfassen unter anderem Angaben zum Bearbeitungszweck, die Kategorie der betroffenen Personen und die Aufbewahrungsdauer der Personendaten. Für die abschliessende Aufzählung der inhaltlichen Mindestanforderungen sollen betroffene Organisationen die genannte Verordnung konsultieren. Die Zewo verlangt von zertifizierten Organisationen, dass sie ihre gesetzlichen Pflichten kennen und entsprechend handeln.

Das verlangt die Zewo bezüglich Bearbeitungsreglement

Es kommen die einleitend im **Zewo-Standard 19 Absatz 1 und Absatz 2** festgehaltenen Grundsätze zur Anwendung. Die Anforderungen der Zewo gehen nicht über die gesetzlichen Rahmenbedingungen hinaus. Ein Bearbeitungsreglement verlangt die Zewo lediglich von Organisationen, welche hierzu gesetzlich verpflichtet sind.

Tipps der Zewo

Organisationen sind gut beraten, falls sie ein Bearbeitungsreglement erstellen müssen, dieses regelmässig zu aktualisieren, ihre Mitarbeitenden und Partner über den Umgang mit besonders schützenswerten Personendaten zu schulen und möglichst auf Profiling mit hohem Risiko zu verzichten.

Zudem ist es ratsam, den Prozess rund um die Erstellung und Aktualisierung des Bearbeitungsreglements zu verschriftlichen und auch die Verantwortlichkeiten klar zu regeln.

Wichtige Prozesse

Auskunft erteilen

Das Datenschutzgesetz räumt betroffenen natürlichen Personen unter anderem das Recht auf Auskunft ein. Demnach können Betroffene von Organisationen Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden. Das Gesetz schreibt in Art. 25 nDSG vor, welche Informationen mittels Auskunft erteilt werden müssen. Dabei handelt es sich beispielsweise um die Identität und die Kontaktdaten der Verantwortlichen, die bearbeiteten Personendaten als solches und den Bearbeitungszweck.

Diese Aufzählung erhebt keinen Anspruch auf Vollständigkeit. Für die abschliessende Auflistung der gesetzlichen Mindestanforderungen soll der erwähnte Gesetzesartikel konsultiert werden. Der Gesetzgeber schreibt die Verwendung eines einheitlichen Auskunftsformulars nicht vor. Die Auskunft soll in der Regel schriftlich erteilt werden, kann jedoch auch auf elektronischem Weg erfolgen. Vorsätzlich falsche oder unvollständige Auskünfte werden mit Bussen bestraft.

Das verlangt die Zewo bezüglich Auskunftserteilung

Es kommen die einleitend im **Zewo-Standard 19 Absatz 1 und Absatz 2** festgehaltenen Grundsätze zur Anwendung. Die Anforderungen der Zewo gehen nicht über die gesetzlichen Rahmenbedingungen hinaus.

Tipps der Zewo

Die Zewo rät Organisationen, ihre internen Prozesse, inkl. Verantwortlichkeiten und Zuständigkeiten, im Umgang mit Auskunftsanfragen klar zu definieren. Allfällige Auskunftsanfragen sollen möglichst zeitnah und kompetent beantwortet werden können. Die Beantwortung der Anfragen von Betroffenen soll i.d.R. innert 30 Tagen und kostenfrei erfolgen. Kann diese Frist nicht eingehalten werden, teilt die Organisation den Gesuchstellenden dies mit und setzt eine neue Frist.

Die Zewo empfiehlt den zertifizierten Organisationen, ein **standardisiertes Auskunftsformular** zu erstellen, um die Auskunftserteilung zu vereinheitlichen und um effiziente interne Abläufe zu etablieren. Nebst dem standardisierten Auskunftsformular ist es ratsam, auch ein einheitliches Vorgehen für den **Identitätsnachweis** der anfragenden Person zu errichten. Bearbeitet eine Organisation keine Personendaten der anfragenden Person, kann sie dennoch nach ihrem Ermessen und Ressourcen eine Negativauskunft erstellen.

Schliesslich empfiehlt die Zewo, eine Person innerhalb der Organisation zu bezeichnen, die für den Datenschutz zuständig ist. Die mit dem Datenschutz beauftragte Person sollte sich datenschutzrechtliches Grundwissen aus öffentlichen Quellen aneignen und bei fachlichen Fragestellungen die Ansprechperson in der Organisation sein.

Umgang mit Datenpannen

In gewissen Fällen müssen Verletzungen des Schutzes personenbezogener Daten, sogenannte Datenpannen, dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) gemeldet werden. Datenpannen können sich beispielsweise aus unbeabsichtigter oder unrechtmässiger Vernichtung, Verlust, Veränderung, unbefugter Offenlegung beziehungsweise unbefugtem Zugang zu personenbezogenen Daten ergeben.

Praktische Beispiele für Verletzungen der Datensicherheit sind Fälle von «Hacking», Verlust von Datenträgern ohne adäquate Verschlüsselung oder der Versand von E-Mails an diverse Empfänger mit unbeabsichtigten Empfängern im CC.

Auf eine Meldung an den EDÖB kann verzichtet werden, wenn die Verletzung des Schutzes der personenbezogenen Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheit der betroffenen

natürlichen Personen führt. Eine Meldung muss möglichst rasch nach Kenntnis über die Verletzung der Datensicherheit erfolgen. Auch betroffene Personen müssen über die Verletzung der Datensicherheit benachrichtigt werden, wenn es zu ihrem Schutz erforderlich ist oder die EDÖB dies verlangt.

Dies bedeutet für Organisationen, dass wenn sie trotz geeigneter technischer und organisatorischer Massnahmen zur Gewährleistung der Sicherheit der Personendaten (d.h. zur Speicherung der Daten, zur Zugänglichkeit, gegen unbefugte Löschung, etc.) eine Datenpanne verzeichnen, ihre Meldepflicht wahrnehmen. Diese besteht, wenn die Verletzung des Schutzes der personenbezogenen Daten voraussichtlich zu einem Risiko für die Rechte und Freiheit der betroffenen natürlichen Personen führt.

Das verlangt die Zewo bezüglich Umgang mit Datenpannen

Es kommen die einleitend im **Zewo-Standard 19 Absatz 1** und **Absatz 2** festgehaltenen Grundsätze zur Anwendung. In diesem Zusammenhang wird zusätzlich auf **Standard 19 Absatz 6** verwiesen.

Die Organisation trifft geeignete technische und organisatorische Massnahmen zur Gewährleistung der Sicherheit der Personendaten (d.h. zur Speicherung der Daten, zur Zugänglichkeit, gegen unbefugte Löschung). Sollte die Datensicherheit verletzt werden, nimmt die Organisation ihre allfälligen Melde- und Informationspflichten wahr.
Zewo-Standard 19 Absatz 6, voraussichtlich ab 01.01.2024 in Kraft

Die Anforderungen der Zewo gehen nicht über die gesetzlichen Rahmenbedingungen hinaus.

Tipps der Zewo

Die potenziellen Risiken sollen bezüglich der Schwere des möglichen Schadens und ihrer Eintrittswahrscheinlichkeit bewertet werden. Wenn ein potenziell hohes Risiko nicht gänzlich ausgeschlossen werden kann, ist es ratsam, die Datenpanne sicherheitshalber zu melden.

Für Organisationen ist es ratsam, eine standardisierte Vorgehensweise zu definieren, die es in Fällen von Datenpannen zu beachten gilt, und somit ein internes Meldeverfahren zu etablieren.

Hinweis: Verletzungen der Datensicherheit können hier dem EDÖB gemeldet werden.
Hinweis: Das Ziel von technischen und organisatorischen Massnahmen (TOM) ist es, die Sicherheit der Daten zu gewährleisten. Vor allem sollen TOM die Daten nur Berechtigten zugänglich machen, die Verfügbarkeit der Daten sicherstellen und die Integrität der Daten vor unberechtigter oder unbeabsichtigter Veränderung wahren.
Zudem sollen TOM die Nachvollziehbarkeit der Datenbearbeitung ermöglichen. Artikel 3 DSV gibt detailliert Aufschluss über die Ausgestaltung und Anforderungen an die TOM. Die gute Nachricht ist, in den meisten Organisationen bestehen bereits TOM.

Löschen und/oder anonymisieren von Personendaten

Artikel 6 Abs. 4 nDSG schreibt vor, dass die Personendaten entweder vernichtet oder anonymisiert werden müssen, sobald ihr Bearbeitungszweck wegfällt. Betroffene Personen können ihre Rechte auf Löschung ausüben und Organisationen zur Löschung ihrer Daten auffordern. Eine Anonymisierung kommt gemäss Gesetz der Löschung gleich. Das Gesetz erfordert grundsätzlich die Löschpflicht der Personendaten, sobald sie für ihren ursprünglichen Zweck nicht mehr benötigt werden. Allerdings gibt es zwei Ausnahmen von der Löschpflicht:

Die Ausnahmen sind: Beweiszwecke und andere überwiegend private Interessen, beispielsweise zur Dokumentation oder zur Erhaltung von Know-how **oder** gesetzliche Aufbewahrungspflichten. Folglich besteht keine absolute Löschpflicht, sondern es werden die Rechte der betroffenen Personen den gesetzlichen Aufbewahrungspflichten und den Interessen der für die Datensammlung verantwortlichen Organisation gegenübergestellt.

Dies bedeutet für Organisationen, dass sie die datenschutzrechtlichen Grundsätze der Erforderlichkeit und der Zweckmässigkeit wahren. Sie sammeln Personendaten sparsam und nur, wenn diese für die Zwecke der Organisation notwendig sind.

Zudem sollten Organisationen ihre Pflichten zur Löschung oder Anonymisierung von Personendaten kennen und die Rechte der betroffenen Personen wahren, indem sie ihrem Wunsch nach Löschung nachkommen, sofern keine Ausnahme von der Löschpflicht besteht.

Das verlangt die Zewo bezüglich Löschung und/oder Anonymisierung von Personendaten

Es kommen die einleitend im **Zewo-Standard 19 Absatz 1** und **Absatz 2** festgehaltenen Grundsätze zur Anwendung. Die Anforderungen der Zewo gehen nicht über die gesetzlichen Rahmenbedingungen hinaus.

Tipps der Zewo

Die Zewo rät Organisationen, im Rahmen ihrer Ressourcen und nach Abwägung möglicher Risiken, ein internes Löschkonzept zu etablieren. Zudem kann es für Organisationen ratsam sein, den Löschprozess ihrer externen Datenverarbeitenden zu kennen. Weiter empfiehlt die Zewo, ein Löschprotokoll zu führen, um erfüllte Löschbegehren von Betroffenen nachzuweisen.

Schliesslich tun Organisationen gut daran, den Datenschutz als einen kontinuierlichen Prozess zu behandeln, in dessen Zentrum das «Datenschutz-Management» steht, und folglich ihre Prozesse, Dokumente und Reglemente periodisch zu überprüfen und wenn nötig anzupassen.

Diese Zewo-Bestimmungen zum Datenschutz gelten weiterhin

Das verlangt die Zewo weiterhin im Standard 19 zum Datenschutz

Die Organisationen dürfen gesammelte Daten und Adressen von natürlichen Personen, insbesondere von Spenderinnen und Spendern, aber auch von anderen Personengruppen, wie z.B. Mitgliedern, Mitarbeitenden, Ehrenamtlichen, Leistungsempfängerinnen und Leistungsempfängern, Angehörigen, interessierten Personen oder weiteren Betroffenen im Sinne des Datenschutzgesetzes, weder verkaufen noch vermieten oder tauschen.

Sie dürfen unter Beachtung der gesetzlichen Rahmenbedingungen neue Adressen von Adressvermittlungsfirmen nutzen. Sie informieren die betroffene Person spätestens einen Monat nach Erhalt angemessen darüber. Dies tun sie beispielsweise mittels Verweises auf ihre Datenschutzerklärung.
Zewo-Standard 19 Absatz 3

Wünschen Personen, dass sie nicht mehr oder weniger oft kontaktiert werden, tragen die Spenden sammelnden Organisationen dem Rechnung und setzen dies schnell und ohne Hindernisse um. Dies gilt soweit möglich auch für Erstkontakte (z.B. Berücksichtigung der Robinsonliste des Schweizer Dialogmarketing Verbands).
Zewo-Standard 19 Absatz 4

Zusammenfassung Pflichtdokumente

Um ihren Umsetzungsbedarf in Bezug auf die Gesetzesänderung im Datenschutzrecht zu evaluieren, können sich zertifizierte Organisationen die folgenden Fragen stellen:

- **Bearbeiten wir personenbezogene Daten von natürlichen Personen?**
- **Haben wir 250 oder mehr Mitarbeitende oder birgt unsere Datenbearbeitung ein hohes Risiko für Betroffene?**
- **Birgt unsere geplante Datenbearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen natürlichen Person, da wir besonders schützenswerte Personendaten bearbeiten oder aufgrund der Art der Datenbearbeitung?**
- **Bearbeiten wir automatisiert und umfangreich besonders schützenswerte Personendaten oder erstellen wir Profiling mit hohem Risiko?**
- **Lassen wir Daten durch Dritte bearbeiten, allenfalls auch im Ausland?**

Basierend auf den obenstehenden Fragen kann somit ermittelt werden, welche gesetzlich vorgeschriebenen Dokumente Organisationen in welchen Fällen erstellen müssen.

Nachfolgend finden Sie einige Beispiele, wann welche gesetzlich vorgeschriebenen Dokumente zu erstellen sind. Die unter Kapitel 2 «Vier empfohlene Dokumente und Prozesse» beschriebenen Dokumente und Prozesse sind keine für alle Verantwortlichen gesetzlich vorgeschriebenen Dokumente. Für sie gilt stets die Verhältnismässigkeit. Dabei sollen Organisationen zwischen potenziellen Risiken und ihren eigenen organisationsinternen Ressourcen abwägen.

Beispiel 1

Findet eine Bearbeitung von Personendaten statt?	☑	erforderliches Dokument	***Ja***	***Datenschutzerklärung***
Gibt es 250 oder mehr Mitarbeitende oder werden Daten mit hohem Risiko verarbeitet?	☒	erforderliches Dokument	*Nein*	Verarbeitungsverzeichnis
Birgt die geplante Datenbearbeitung ein hohes Risiko?	☒	erforderliches Dokument	*Nein*	Datenschutz-Folgenabschätzung
Finden umfangreiche, automatisierte Bearbeitungen von besonders schützenswerten Personendaten oder Profiling mit hohem Risiko statt?	☒	erforderliches Dokument	*Nein*	Bearbeitungsreglement

Beispiel 2

Findet eine Bearbeitung von Personendaten statt?	☑	erforderliches Dokument	***Ja***	***Datenschutzerklärung***
Gibt es 250 oder mehr Mitarbeitende oder werden Daten mit hohem Risiko verarbeitet?	☑	erforderliches Dokument	***Ja***	***Verarbeitungsverzeichnis***
Birgt die geplante Datenbearbeitung ein hohes Risiko?	☑	erforderliches Dokument	***Ja***	***Datenschutz-Folgenabschätzung***
Finden umfangreiche, automatisierte Bearbeitungen von besonders schützenswerten Personendaten oder Profiling mit hohem Risiko statt?	☑	erforderliches Dokument	***Ja***	***Bearbeitungsreglement***

Beispiel 3

Findet eine Bearbeitung von Personendaten statt?	☑	erforderliches Dokument	***Ja***	***Datenschutzerklärung***
Gibt es 250 oder mehr Mitarbeitende oder werden Daten mit hohem Risiko verarbeitet?	☒	erforderliches Dokument	Nein	Verarbeitungsverzeichnis
Birgt die geplante Datenbearbeitung ein hohes Risiko?	☒	erforderliches Dokument	Nein	Datenschutz-Folgenabschätzung
Finden umfangreiche, automatisierte Bearbeitungen von besonders schützenswerten Personendaten oder Profiling mit hohem Risiko statt?	☒	erforderliches Dokument	Nein	Bearbeitungsreglement
Gibt es eine Übertragung der Bearbeitung von Personendaten an Dritte?	☒		Nein	Keine Überprüfung AVV

Beispiel 4

Findet eine Bearbeitung von Personendaten statt?	☑	erforderliches Dokument	***Ja***	***Datenschutzerklärung***
Gibt es 250 oder mehr Mitarbeitende oder werden Daten mit hohem Risiko verarbeitet?	☒	erforderliches Dokument	Nein	Verarbeitungsverzeichnis
Birgt die geplante Datenbearbeitung ein hohes Risiko?	☑	erforderliches Dokument	***Ja***	***Datenschutz-Folgenabschätzung***
Finden umfangreiche, automatisierte Bearbeitungen von besonders schützenswerten Personendaten oder Profiling mit hohem Risiko statt?	☒	erforderliches Dokument	Nein	Bearbeitungsreglement

Beispiel 5

Findet eine Bearbeitung von Personendaten statt?	☑	erforderliches Dokument	***Ja***	***Datenschutzerklärung***
Gibt es 250 oder mehr Mitarbeitende oder werden Daten mit hohem Risiko verarbeitet?	☒	erforderliches Dokument	Nein	Verarbeitungsverzeichnis

Birgt die geplante Datenbearbeitung ein hohes Risiko?	☒	erforderliches Dokument	Nein	*Datenschutz-Folgenabschätzung*
Finden umfangreiche, automatisierte Bearbeitungen von besonders schützenswerten Personendaten oder Profiling mit hohem Risiko statt?	☑	erforderliches Dokument	***Ja***	**Bearbeitungsreglement**

Disclaimer

Diese Umsetzungshilfe ist keine Detailbeurteilung des Umsetzungsbedarfs von individuellen Organisationen im Hinblick auf das revidierte Datenschutzgesetz. Vielmehr versucht diese Umsetzungshilfe, Organisationen des Nonprofit-Sektors auf die angepasste Gesetzeslage vorzubereiten und zu sensibilisieren. Die Umsetzungshilfe beantwortet keine Detailfragen und erhebt keinen Anspruch auf Vollständigkeit. Im Zusammenhang mit spezifischen Fragestellungen wird empfohlen, sich an Datenschutzexpertinnen und -experten zu wenden.

Glossar

Auftragsverarbeitung	Im Rahmen einer Auftragsverarbeitung wird die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten, sprich die Datenverarbeitung, an Dritte übertragen. Beispiele hierfür sind Marketingaktionen, Kundenumfragen und Newsletter-Versände durch Dritte.
Auskunftspflicht	Jede Organisation muss auf Gesuch einer natürlichen Person Auskunft darüber erteilen, ob Daten über sie bearbeitet werden. Sollte dies der Fall sein, muss die Organisation der Person Zugang zu ihren Daten ermöglichen.
Aspekte der Persönlichkeit	Mit Aspekten der Persönlichkeit sind unter anderem Bereiche der Persönlichkeit wie Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel einer natürlichen Person gemeint.
Bearbeitung von Personendaten	Die Bearbeitung von Personendaten umfasst jeglichen Umgang mit Personendaten, beispielsweise das Beschaffen, Verwenden, Aufbewahren, Umarbeiten, Bekanntgeben oder Vernichten von personenbezogenen Daten.

Besonders schützenswerte Personendaten	Daten über: - ethnische Herkunft und Rasse - politische Meinung - Gesundheitsdaten - biometrische Daten - genetische Daten - religiöse oder weltanschauliche Überzeugungen - sexuelle Orientierung
Löschkonzept	Ein Löschkonzept ist eine Erklärung beziehungsweise eine Beschreibung, wann und wie personenbezogene Daten innerhalb einer Organisation gelöscht werden.
Löschprotokoll	Mittels Löschprotokoll kann in allgemeiner Form festgehalten werden, an welchen Tagen welche Daten gelöscht wurden.
Personendaten	Personendaten sind Daten, welche sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Diese theoretische Umschreibung kann in der Praxis sehr umfassend sein. Unter Umständen kann es sich bereits bei einer IP-Adresse um Personendaten handeln.
Profiling mit hohem Risiko	Im revidierten Datenschutzgesetz wird mit dem Begriff «Profiling mit hohem Risiko» jedes Vorgehen erfasst, in dem die automatisierte Bearbeitung von Personendaten bestimmte persönliche Aspekte einer natürlichen Person vorhersagt oder bewertet.
TOM	Geeignete technische und organisatorische Massnahmen zur Wahrung einer dem Risiko angemessenen Datensicherheit. Diese können von Backups über geeignete Passwörter bis hin zu Firewalls reichen.
Verantwortliche	Verantwortliche im Sinne des Datenschutzrechts können natürliche oder juristische Personen aber auch Behörden oder andere Organisationen und Stellen sein, welche über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten bestimmen.

Verjährungsfristen	Verjährungsfristen ergeben sich aus den gesetzlichen Aufbewahrungsfristen. Sie belaufen sich in der Regel auf 10 Jahre mit gewissen gesetzlichen Ausnahmen.

Quellen und nützliche Links

Datenschutzgesetz: https://www.fedlex.admin.ch/eli/cc/2022/491/de

Datenschutzverordnung: https://www.newsd.admin.ch/newsd/message/attachments/75620.pdf
Dsat, Datenschutz Self Assessment Tool: https://dsat.ch/
Fairpicture, Ein Leitfaden zum datenschutzkonformen Umgang mit Bildern und Videos: Whitepaper Datenschutz Visuelle Kommunikation (fairpicture.org)
FAQ Datenschutzrecht Admin: https://www.newsd.admin.ch/newsd/message/attachments/75632.pdf
Onlinekommentar: Home (onlinekommentar.ch)
ProFonds, Datenschutz: https://www.profonds.org/de/interessenwahrung/das-neue-datenschutzgesetz-dsg/