Centre Patronal

Stand, 26. September 2023

FAQ revidiertes Datenschutzgesetz – Was muss ich als Unternehmer wissen?

Das revidierte Datenschutzgesetz (DSG) trat am 1. September 2023 in Kraft. Das DSG betrifft u.a. jedes Schweizer Unternehmen, jeden Verein und jede Stiftung, die bewusst oder unbewusst personenbezogene Daten bearbeiten. Dazu gehören auch Arbeitgeber.

Wir stellen fest, dass die Verunsicherung im Zusammenhang mit den Änderungen des DSG gross ist. Das Centre Patronal bietet insbesondere mit Blick auf Fragestellungen, die sich Arbeitgebern im Zusammenhang mit dem neuen Datenschutzgesetz stellen, Unterstützung in Form eines Webinars «Revidiertes Datenschutzgesetz – Seien Sie rechtzeitig à jour». Zusätzlich haben wir die wichtigsten Grundlagen und Änderungen in einem FAQ zusammengefasst, um Ihnen den Einstieg in die Thematik zu erleichtern.

In unseren FAQ beleuchten wir diese und weitere mögliche arbeitsrechtliche Fragen-stellungen mit dem Ziel, Klarheit zu schaffen und praktische Handlungsempfehlungen abzugeben.

Die Ausführungen sind bewusst einfach und pragmatisch gehalten und als Orientierungshilfe zu verstehen. Sie ersetzen nicht eine eingehende juristische Prüfung im Einzelfall. Zudem weisen wir darauf hin, dass sich das FAQ auf die Bearbeitung von Personendaten durch private Verantwortliche fokussiert. Zwei zentrale Punkte bei der Umsetzung sind die Transparenz und die Dokumentation.

1. Grundlagen

Fragen	Antworten
1.1 **Wo kann ich mich informieren?**	Nützliche Informationen finden Sie u.a. auf der Website des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (vgl. Website EDÖB; Häufige Fragen zum Datenschutz).

	Das Bundesamt für Justiz hat auf seiner Website ebenfalls ein FAQ aufgeschaltet, das zu einem besseren Verständnis des DSG beitragen soll (vgl. Website BJ). Der EDÖB hat auf seiner Website ein Formular aufgeschaltet, mit dem Datensicherheitsverletzungen gemeldet werden können (vgl. Online-Dienst zur Meldung von Datensicherheitsverletzungen). Die Swisscom bietet KMU einen kostenlosen IT-Security-Check bei dem Sie das Sicherheitsniveau Ihrer IT prüfen können (vgl. Swisscom IT-Security-Check für KMU). Die Staaten, Gebiete, spezifische Sektoren in einem Staat und internationale Organe mit einem angemessenen Datenschutz sind in Anhang 1 DSV aufgeführt. Mit Blick auf die konkreten Fragestellungen, die sich Arbeitgebern im Zusammenhang mit dem neuen Datenschutzgesetz stellen, hat Centre Patronal das Webinar: «Revidiertes Datenschutzgesetz - Seien Sie rechtzeitig à jour» im Angebot.
1.2 **Was hat sich im Vergleich zum alten Datenschutzgesetz geändert?**	Wichtig zu wissen ist, dass die bisherigen Datenschutzgrundsätze unverändert weitergelten. D.h. wenn Sie als Arbeitgeber bereits nach altem Recht fit im Umgang mit Datenschutzfragen waren, wird dies auch nach neuem Recht rasch der Fall sein. Das DSG ist gegenüber dem bisherigen Stand erheblich umfangreicher geworden. Es beinhaltet u.a. neue Begriffe und Rollen und definiert neue Aufgaben (vgl. dazu die nachfolgenden Fragen). Eine wichtige Änderung ist zudem, dass das DSG neu nur noch Personendaten von natürlichen Personen schützt (Art. 2 Abs. 1 DSG). D.h. Vereine und Stiftungen fallen nicht mehr in den Schutzbereich des Gesetzes, sondern müssen - unter Strafandrohung nach Art. 60 ff. DSG - als Datenbearbeiterinnen eine Reihe von Pflichten erfüllen.
1.3 **Welche Grundsätze sind bei der Bearbeitung von Personen-daten zu beachten?**	Wie bereits erwähnt, hat sich in Bezug auf die Grundsätze der Bearbeitung von Personendaten nichts Wesentliches verändert:

	Personendaten müssen rechtmässig bearbeitet werden (Art. 6 Abs. 1 DSG). D.h. die Bearbeitung darf insb. nicht gegen spezifische gesetzliche Bestimmungen verstossen. Zentral ist, dass die Bestimmungen des DSG eingehalten werden. Die Bearbeitung muss nach Treu und Glauben erfolgen und verhältnismässig sein (Art. 6 Abs. 2 DSG). Die Datenbearbeitung muss für Betroffene nachvollziehbar sein. M.a.W. muss sie wissen oder erkennen, welche Daten zu welchem Zweck bearbeitet werden. Der Grundsatz der Verhältnismässigkeit setzt voraus, dass nur Daten bearbeitet werden, die für den Zweck der Bearbeitung geeignet, erforderlich und für die betroffene Person zumutbar sind. Personendaten dürfen nur zu einem bestimmten und für die betroffene Person erkennbaren Zweck beschafft werden. Sie dürfen nur so bearbeitet werden, dass es mit diesem Zweck vereinbar ist (Art. 6 Abs. 3 DSG). Personendaten werden vernichtet oder anonymisiert, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind (Art. 6 Abs. 4 DSG). Wer Personendaten bearbeitet, muss sich über deren Richtigkeit vergewissern (Art. 6 Abs. 5 DSG). *Wenn einer oder mehrere Bearbeitungsgrundsätze nicht erfüllt sind, bedarf es für die Bearbeitung einen Rechtfertigungsgrund (vgl. Art. 30 ff. DSG). Ein typischer Rechtfertigungsgrund ist die Einwilligung durch die betroffene Person (vgl. Art. 31 i.V.m. Art. 6 Abs. 7 DSG).*
1.4 Was sind «Personendaten» und was versteht man unter dem Begriff «Bearbeiten»?	Personendaten sind alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen.
1.5 Wann spricht man von besonders schützenswerten Personendaten?	Hierbei handelt es sich um • Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten;

	• Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie; • Genetische Daten; • Biometrische Daten, die eine natürliche Person eindeutig identifizieren; • Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen; • Daten über Massnahmen der sozialen Hilfe.
1.6 Welche Rollen sind im Zusammenhang mit der Bearbeitung von Personendaten auseinanderzuhalten?	Für das Verständnis ist es wichtig, dass Sie die verschiedenen Rollen und Institutionen des DSG kennen. Im Einzelnen gilt es folgende Rollen auseinanderzuhalten: • Betroffene Person: Natürliche Person, über die Personendaten bearbeitet werden (Art. 5 lit. a DSG). • Verantwortlicher: Private Person (natürliche oder juristische Person) oder Bundesorgan, die oder das allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung entscheidet (Art. 5 lit. j DSG). Verantwortlicher kann somit beispielsweise die «X AG, handelnd durch ihre Geschäftsleitung» sein. • Auftragsbearbeiter: Private Person (natürliche oder juristische Person) oder Bundesorgan, die oder das im Auftrag des Verantwortlichen Personendaten bearbeitet. Auftragsbearbeiter sind Dienstleister, die gestützt auf einen Outsourcingvertrag Personendaten für den Verantwortlichen bearbeiten. • Datenschutzberater: Private Verantwortliche können einen Datenschutzberater ernennen. Er ist Anlaufstelle für die betroffenen Personen und für die Behörden, die in der Schweiz für den Datenschutz zuständig sind (vgl. Art. 10 DSG). Im Unterschied zur Datenbearbeitung durch Bundesorgane ist die Ernennung eines Datenschutzberaters für private Verantwortliche freiwillig.

	• EDÖB (Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter): Er beaufsichtigt die Anwendung der bundesrechtlichen Datenschutzvorschriften. Er kann von Amtes wegen oder auf Anzeige hin eine Untersuchung wegen Datenschutzverletzung eröffnen und hat Verfügungskompetenz.
1.7 Wann falle ich in den Anwendungsbereich der Europäischen Datenschutzverordnung (DSGVO)?	Für Schweizer Unternehmen gilt in erster Linie Schweizer Recht und damit das DSG. Die europäische Datenschutzverordnung (DSGVO) ist nicht direkt anwendbar auf Schweizer Unternehmen. In bestimmten Situationen kann es jedoch durchaus vorkommen, dass ein Schweizer Unternehmen auch die Vorgaben der DSGVO einhalten muss. Massgebend sind die folgenden beiden Kriterien: Kriterium der Niederlassung: Der Verantwortliche oder Auftragsbearbeiter hat seine Niederlassung in der Europäischen Union. Kriterium des Zielmarktes: Die Niederlassung des Verantwortlichen befindet sich ausserhalb der Europäischen Union, aber die Bearbeitung betrifft Waren oder Dienstleistungen, die für Personen in der Union bestimmt sind, oder die Bearbeitung betrifft die Beobachtung des Verhaltens einer betroffenen Person, soweit deren Verhalten in der Union erfolgt. Weiterführende Informationen finden Sie im FAQ des EDÖB «Häufige Fragen zum Datenschutz» unter DSGVO.

2. Neue Aufgaben und Begriffe bei der Bearbeitung von Personendaten

2.1 Was ist ein Verzeichnis der Bearbeitungstätigkeiten bzw. Dateninventar und wann muss ein solches erstellt werden?	Der Verantwortliche und der Auftragsbearbeiter führen je ein Verzeichnis über ihre Bearbeitungstätigkeiten (Art. 12 DSG). Das Verzeichnis beinhaltet im Wesentlichen die Information: Wer bearbeitet welche Daten zu welchem Zweck?

	Unternehmen, die weniger als 250 Mitarbeitende beschäftigen und deren Datenbearbeitung ein geringes Risiko für die Verletzung der Persönlichkeit der betroffenen Personen mit sich bringt, können auf die Erstellung eines Verzeichnisses verzichten. Gemäss Art. 24 DSV ist von keinem hohen Risiko auszugehen, wenn weder besonders schützenswerte Personendaten in grossem Umfang bearbeitet werden noch ein Profiling mit hohem Risiko durchgeführt wird. Auch wenn ein Unternehmen von der Pflicht zur Erstellung eines Bearbeitungsverzeichnisses befreit ist, kann ein solches bei der Erfüllung von anderweitigen Datenschutzpflichten helfen. Letztlich dient es dem Verständnis wer im Unternehmen, welche Daten zu welchem Zweck bearbeitet.
2.2 Was ist unter der Informationspflicht zu verstehen?	Die Informationspflicht (Art. 19 ff. DSG) ist eine zentrale Pflicht, um den Grundsatz der Transparenz sicherzustellen. Demnach muss der Verantwortliche die betroffene Person angemessen über die Beschaffung von Personendaten informieren. Diese Informationspflicht gilt auch, wenn die Daten nicht bei der betroffenen Person selbst beschafft werden. Die Informationspflicht wurde von den bisher betroffenen besonders schützenswerten Personendaten und Persönlichkeitsprofilen (Art. 14 aDSG) auf alle Personendaten ausgeweitet. Art. 19 Abs. 2 DSG definiert den Mindestinhalt, den der Verantwortliche der betroffenen Person bei der Beschaffung mitteilen muss. Das Gesetz schreibt nicht vor, in welcher Form die betroffene Person informiert werden muss. In der Praxis geschieht dies i.d.R. in Form einer Datenschutzerklärung auf der Website. Zudem sollte eine separate interne Datenschutzerklärung für das Personal vorgesehen werden.
2.3 Wann ist eine sog. Datenschutz-Folgenabschätzung (DSFA) erforderlich?	Bei jeder Bearbeitung von Personendaten muss sich der Verantwortliche vorgängig überlegen, welche Risiken die Bearbeitung für Betroffene haben könnte. Art. 22 DSG sieht nämlich vor, dass vorgängig eine DSFA zu erstellen ist, wenn eine Bearbeitung ein hohes Risiko für

	die Persönlichkeit oder die Grundrechte der betroffenen Person haben könnte. Ein hohes Risiko ergibt sich insb. bei der Verwendung von neuen Technologien, aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung. Es liegt namentlich vor: • Bei der umfangreichen Bearbeitung von besonders schützenswerten Personendaten i.S.v. Art. 5 lit. c DSG. • Wenn systematisch umfangreiche öffentliche Bereiche überwacht werden. Die DSFA enthält eine Beschreibung der geplanten Bearbeitung, eine Bewertung der Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person sowie die Massnahmen zum Schutz der betreffenden Risiken. Es ist empfehlenswert, nicht nur die eigentliche Durchführung der DSFA zu dokumentieren, sondern auch die Überlegungen, ob eine solche durchgeführt werden muss und zu welchem Ergebnis man gekommen ist (sog. Schwellenwertanalyse).
2.4 Was ist unter Datensicherheitsverletzung zu verstehen und wann ist eine solche meldepflichtig?	Eine Datensicherheitsverletzung liegt vor, wenn Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden (Art. 5 lit. h DSG). Der Verantwortliche muss dem EDÖB so rasch als möglich eine Verletzung der Datensicherheit melden, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt (Art. 24 DSG). Geschieht die Verletzung beim Auftragsbearbeiter, hat dieser den Verantwortlichen so schnell wie möglich zu informieren. Der Verantwortliche muss die betroffene Person informieren, wenn es zu ihrem Schutz erforderlich ist oder es der EDÖB verlangt. Im Unternehmen sind daher Prozesse und Verantwortlichkeiten zu etablieren, dass Datensicherheitsverletzungen erkannt, potenzielle Risiken eruiert und die ggf. notwendigen Meldungen abgesetzt werden. Der EDÖB hat auf seiner Website ein Formular aufgeschaltet, mit dem Datensicherheitsverletzungen gemeldet werden können (vgl. Online-Dienst zur Meldung von Datensicherheitsverletzungen)

2.5 Was heisst «Privacy by Design» und «Privacy by Default»?

Hier geht es um Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen (vgl. Art. 7 DSG). Der Verantwortliche ist verpflichtet, die Datenbearbeitung technisch und organisatorisch so auszugestalten, dass die Datenschutzvorschriften, insb. die Datenschutzgrundsätze, eingehalten werden (vgl. Frage unter Ziff. 1.3). Konkretisiert wird die Verpflichtung durch die Grundsätze «Privacy by Design» und «Privacy by Default»:

Privacy by Design: Die technischen und organisatorischen Massnahmen (sog. «TOMs») müssen insbesondere dem Stand der Technik, der Art und dem Umfang der Datenbearbeitung sowie dem Risiko, das die Bearbeitung für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringt, angemessen sein (Art. 7 Abs. 2 DSG).

Privacy by Default: Der Verantwortliche ist verpflichtet, mittels geeigneter Voreinstellungen sicherzustellen, dass die Bearbeitung der Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt ist, soweit die betroffene Person nicht etwas anderes bestimmt (Art. 7 Abs. 3 DSG).

- Typische TOMs sind z.B.:
- Zugriffsbeschränkungen;
- Beschränkung der Aufbewahrungsdauer;
- Sicherstellung der Datensicherheit (Firewalls, MFA, Alarmanlagen, usw.);
- Pseudonymisierung und Datenverschlüsselung;
- Protokollierung, Backups, Updates;
- Nutzerrechte definieren und kontrollieren;
- Überprüfung auf Richtigkeit;
- Weisungen, Schulungen von Mitarbeitenden zum Thema Datenschutz usw.

Die Swisscom bietet KMU einen kostenlosen IT-Security-Check bei dem Sie das Sicherheitsniveau Ihrer IT prüfen können (vgl. Swisscom IT-Security-Check für KMU).

2.6 Was gilt es bei den Betroffenenrechten (Auskunfts-, Lösch- und Berichtigungsrecht) zu beachten?	Jede Person kann vom Verantwortlichen Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden (vgl. Art. 25 DSG). Trifft dies zu, kann sie Auskunft über die Personendaten als solche und zusätzliche Informationen verlangen (Zweck der Bearbeitung, Aufbewahrungsdauer, Empfänger usw.). Betroffene können verlangen, dass unrichtige Personendaten berechtigt werden oder (wenn eine Berichtigung nicht möglich ist) gelöscht werden (vgl. Art. 32 DSG). Insb. hinsichtlich des Auskunftsrechts empfiehlt es sich, einen systematischen Prozess zur Beantwortung solcher Begehren zu etablieren. Im Zentrum stehen dabei folgende Fragen: Wo gehen Auskunftsersuchen ein? Wer prüft das Gesuch und koordiniert die Bearbeitung? Wer stellt die Einhaltung der gesetzlichen Frist sicher?
2.7 Wann liegt ein sog. Profiling vor?	Als Profiling gilt jede Art der automatisierten Bearbeitung von Personendaten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insb. um Aspekte bzgl. Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Personen zu analysieren oder vorherzusagen. Wenn das Profiling zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt, indem es zu einer Verknüpfung von Daten führt, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt, liegt ein sog. Profiling mit hohem Risiko vor (vgl. Art. 5 lit. f und g DSG). Bei einem Profiling mit hohem Risiko durch eine private Person ist eine ausdrückliche Einwilligung der Betroffenen erforderlich (Art. 6 Abs. 7 DSG).
2.8 Wann spricht man von automatisierten Einzelentscheidung?	Hier geht es um eine Entscheidung, die ausschliesslich auf automatisierten Grundlagen basiert. D.h. es kommt im Entscheidungsprozess zu keiner Intervention durch eine natürliche Person. Ist die automatisierte Einzelentscheidung mit Rechtsfolgen für die betroffene Person verbunden oder wird letztere dadurch erheblich beeinträchtigt, muss der Verantwortliche über die Entscheidung informieren (vgl. Art. 21 DSG).

3. Organisatorische Anforderungen

3.1 Welche organisatorischen Anforderungen stellt das DSG an mein Unternehmen?	Das DSG stellt keine spezifischen Anforderungen an die Unternehmensorganisation. Allerdings ist zwecks Einhaltung der Datenschutzvorschriften die Implementierung von einigen organisatorischen Grundsätzen empfehlenswert. In den meisten Fällen lohnt es sich, innerhalb des Unternehmens jemanden zu bestimmen, der für Datenschutzfragen zuständig ist. Dies insb. deshalb, um erforderliche Massnahmen zu koordinieren und im Unternehmen die notwendige Beachtung des Datenschutzthemas sicherzustellen. Zur Erfüllung von gewissen neuen Aufgaben empfiehlt es sich, geeignete Prozesse zu etablieren. Das gilt insb. für: • die Erfüllung der Meldepflicht bei Datensicherheitsverletzungen; • die Umsetzung von Betroffenenrechten (Auskunfts-, Lösch- und Berichtigungsrechte).
3.2 Welche Massnahmen drängen sich zur Sicherstellung datenschutzrechtlicher Compliance auf?	Dateninventar: Im Rahmen einer Bestandesaufnahme gilt es festzustellen, welche Daten wo gespeichert werden, wer sie zu welchem Zweck bearbeitet und wie Zugriffsrechte geregelt sind. Hierzu drängt sich die Erstellung eines Dateninventars auf, unabhängig davon, ob eine Pflicht zur Erstellung besteht oder nicht. Informationspflicht: Auf Grundlage dieser Bestandesaufnahme ist zu prüfen, ob im Zuge der Beschaffung von Personendaten ausreichend informiert wird. Dasselbe gilt, wenn in Ihrem Unternehmen automatisierte Einzelentscheidungen getroffen werden. Sensibilisierung der Mitarbeitenden: Mitarbeitende sind in Bezug auf Datenschutzpflichten und -risiken zu schulen. Dies einerseits, um die Einhaltung der Datenschutzpflichten sicherzustellen und andererseits allfällige Datensicherheitsverletzungen zu erkennen.

Bearbeitung durch Dritte: Verschaffen Sie sich einen Überblick über eingebundene Auftragsdatenbearbeiter und prüfen Sie, ob die erforderlichen Outsourcingverträge abgeschlossen wurden. Wichtig ist, dass der Auftragsbearbeiter die Anforderungen an die Datensicherheit gewährleistet und Sie als Verantwortlicher periodische Überprüfungen vornehmen (lassen) können.

Bekanntgabe ins Ausland: Prüfen Sie, ob Personendaten ins Ausland übermittelt werden. Ist dies der Fall, ist die Gleichwertigkeit des Persönlichkeitsschutzes gemäss Art16 DSG sicherzustellen. Die Staaten, Gebiete, spezifische Sektoren in einem Staat und internationale Organe mit einem angemessenen Datenschutz sind in Anhang 1 DSV aufgeführt. Gewährleistet der Empfängerstaat keinen angemessenen Datenschutz, sind zusätzliche Massnahmen zu treffen wie beispielsweise spezielle vertragliche Vereinbarungen oder das Einholen von Einwilligungen.

DSFA: Es ist sicherzustellen, dass bei geplanten Datenbearbeitungsvorgängen eine Risikoabschätzung vorgenommen oder zumindest eine negative Schwellenwertanalyse durchgeführt und dokumentiert wird.

TOMs: Prüfen Sie, ob die TOMs zur Datensicherheit mit Blick auf die bearbeiteten Personendaten und die damit verbundenen Risiken angemessen sind. Es bietet sich an, die Massnahmen im Dateninventar aufzuführen. Eine wichtige Rolle bei den TOMs spielt die IT-Sicherheit. Daher empfiehlt es sich, einen IT-Spezialisten in die Umsetzung einzubeziehen.

Meldepflicht: Stellen Sie durch einen geeigneten Prozess sicher, dass die Meldepflicht bei Datensicherheitsverletzungen sowohl vom Ablauf her als auch inhaltlich erfüllt wird.

Betroffenenrechte: Stellen Sie durch einen geeigneten Prozess sicher, dass die Betroffenenrechte fristgerecht umgesetzt werden.

4. Strafbestimmungen

4.1 Wann drohen strafrechtliche Sanktionen?	• Wenn der Verantwortliche die Informationspflicht bei der Beschaffung von Personendaten verletzt (Art. 19 DSG), indem er vorsätzlich nicht, falsch oder unvollständig informiert; • Wenn der Verantwortliche die Informationspflicht bei einer automatisierten Einzelfallentscheidung verletzt (Art. 21 DSG), indem er vorsätzlich nicht, falsch oder unvollständig informiert. • Wenn der Verantwortliche im Rahmen des Auskunftsrechts (Art. 25-27 DSG) vorsätzlich nicht, falsch oder unvollständig Auskunft erteilt. • Wenn die private Person dem EDÖB im Rahmen einer Untersuchung vorsätzlich falsche Informationen erteilt oder vorsätzlich die Mitwirkung verweigert. • Wenn vorsätzlich Personendaten ins Ausland bekanntgegeben werden, ohne dass die Voraussetzungen erfüllt sind. • Wenn die Datenbearbeitung einem Auftragsbearbeiter vorsätzlich übertragen wird, ohne dass die Voraussetzungen hierzu erfüllt sind. • Wenn die Datenbearbeitung an einen Dritten übertragen wird, ohne dass dieser die Datensicherheit gewährleisten kann. • Wenn die Mindestanforderungen an die Datensicherheit vorsätzlich verletzt werden. • Vorsätzliche Verletzungen der beruflichen Schweigepflicht. • Vorsätzliche Missachtung von Verfügungen.
4.2 Welche Strafe droht bei einer strafbaren Verletzung?	Die Verletzung bestimmter datenschutzrechtlicher Pflichten kann gemäss Art. 60 ff. DSG zu einer Busse von bis zu CHF 250'000.- führen. Die Verfolgungsverjährung beträgt 5 Jahre (Art. 66 DSG).
4.3 Muss ich auch bei fahrlässigem Handeln mit einer Strafe rechnen?	Nein. Bestraft wird nur eine vorsätzliche Begehung der Tat auf Antrag hin (kein Offizialdelikt).

Stand, 26. September 2023