AVENIQ

Neues Datenschutzgesetz:

Werden bald Mitarbeitende statt Firmen zur Kasse gebeten?

Referent: Meti Rudaj
Senior Cyber Security Consultant bei Aveniq

Baden, 14. Juni 2023

Herzlich Willkommen

Meti Rudaj, Senior Cyber Security Consultant

- Seit 12 Jahren im Bereich Cyber Security tätig
- Fachthemen: Datenschutz und Informationssicherheit
- Begleitung von Kunden bei der Umsetzung von Datenschutzthemen im Bereich der Informationstechnologie

Kontakt: meti.rudaj@aveniq.ch

Inhalt der Präsentation

1. Das neue Schweizer Datenschutzgesetz
2. Die wesentlichen Unterschiede zur europäischen DSGVO
3. Verbindung zwischen IT und Datenschutz
4. Handlungsempfehlungen für das Gesundheitswesen:
   Vorbereitung für den 1. September 2023
5. Konsequenzen bei Nichtanwendung: Persönliche Strafbarkeit

Das neue Schweizer Datenschutzgesetz

Um was geht es?

Die Fakten

Um was geht es?

1992

Schweizer Datenschutzgesetz tritt in Kraft

15.05.2018

DSGVO tritt in Kraft
Firmen im EU-Raum werden mit hohen Bussen für Daten-schutzverletzungen bestraft

Erste Bussen für Schweizer Firmen

2018-2020

Schweizer Firmen mit Bezug zur EU stellen auf die DSGVO um

25.09.2020

Entwurf des neuen Datenschutzgesetzes
Die ersten Firmen bereiten sich vor

01.09.2023

Neues Datenschutzgesetz tritt in Kraft

Erste Bussen für Schweizer Firmen ??

Verstoss gegen die EU-DSGVO

Datenschutzbehörde verdonnert Meta zu Busse von 390 Millionen Euro

Do 05.01.2023 - 10:44 Uhr
von René Jaun und msc

Die von Meta betriebenen Dienste Facebook und Instagram zeigen ihren Usern personalisierte Werbung an. Die Zustimmung dafür holen sie sich über die AGB. Damit verstossen sie gegen die EU-DSGVO, findet die irische Datenschutzbehörde, und büsst Meta mit 390 Millionen Euro.

(Quelle: www.parlament.ch)

1. September 2022 - Nach langem Hin und Her ist es endlich soweit – es gibt ein festes Datum für das Inkrafttreten des totalrevidierten Schweizer Datenschutzgesetzes: Ab dem 1. September 2023 gilt das Schweizer DSGVO-Pendant.

Die Fakten

Was sind personenbezogene Daten?

Personenbezogenen Daten

- Alle Informationen, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen

Betroffene Person

- Natürliche Person, über die Informationen bearbeitet werden

Besonders schützenswerte Daten

- Informationen über Religion, politische oder weltanschauliche Einstellung
- Informationen zu Gesundheitszustand, Rassenzugehörigkeit oder sozialer Status
- Informationen über administrative oder strafrechtliche Verfolgung und Sanktionen

Das neue Schweizer Datenschutzgesetz
Was ändert sich?

Das neue Schweizer Datenschutzgesetz

Was ändert sich?

Die Revision des DSG zielt auf eine Harmonisierung mit der EU Datenschutz-Grundverordnung (EU DSGVO) ab.
Die Grundprinzipien des schweizerischen Datenschutzrechts bleiben aber unverändert.

Hervorzuheben sind folgende Neuerungen:

Geltungsbereich	• Schutz **natürlicher** Personendaten
Erweiterter Umfang	• Genetische und biometrische Daten gelten als **besonders schützenswert**
Verbesserte Transparenz	• Weitergehende **Informationspflichten**
Bearbeitungs-verzeichnis	• Verpflichtend ein Verzeichnis der **Bearbeitungstätigkeiten** zu führen
Datenschutz-folgenabschätzung	• DSFA muss bei Datenbearbeitung mit **hohem Risiko** durchgeführt werden
Profiling	• Automatisierte Datenbearbeitung, um bestimmte **persönliche Aspekte** einer Person zu bewerten
Schnelle Meldung an den EDÖB	• Verletzungen der Datensicherheit, müssen dem **EDÖB so rasch als möglich** gemeldet werden
Privacy-by-Design und **Privacy-by-Default**	• Datenschutz durch **Technik** und datenschutzfreundliche **Voreinstellungen**

Das neue Schweizer Datenschutzgesetz
Was bleibt unverändert?

Im Unterschied zur DSGVO, die für jede Datenbearbeitung eine Rechtsgrundlage verlangt, ändert sich die Art und Weise der Datenbearbeitung nach nDSG nicht grundlegend.

Wie bisher ist für die Bearbeitung von Personendaten durch private Unternehmen im Unterschied zur DSGVO keine Einwilligung oder ein anderer Rechtfertigungsgrund nötig, sofern:

Keine Einwilligung verpflichtend

- **Transparenz, Zweckbindung, Verhältnismässigkeit** und **Datensicherheit** werden eingehalten
- Betroffene Person **widerspricht** der Bearbeitung **nicht**
- **Dritten** werden keine Personendaten mitgeteilt

Einwilligung verpflichtend

- Bearbeitung von **besonders schützenswerten Personendaten**
- Nutzung von **Profiling**
- Für **Behörden**

Die wesentlichen Unterschiede zur europäischen DSGVO

Die wesentlichen Unterschiede zur europäischen DSGVO

Ernennung eines Datenschutzbeauftragten	Freiwillig aber empfohlen	Pflicht
Meldepflicht bei Datenschutzverletzungen	Umgehend	Innerhalb von 72 Stunden
Geldstrafen	Bis CHF 250’000 gegen natürliche Personen	Bis 20 Mio € oder 4 % des globalen Umsatzes gegen juristische Personen
Einwilligung	Nur für Behörden, besonders schützenswerte Daten und Profiling	Für jedwede Personendaten
Datenschutzfolgenabschätzung	Verpflichtend bei bestimmter risikoreicher Datenbearbeitung	Verpflichtend bei risikoreicher Datenbearbeitung mit detaillierten Anforderungen
Verzeichnis der Bearbeitungstätigkeiten	Verpflichtend mit einzelnen Ausnahmen	Verpflichtend mit Formvorschriften

Verbindung zwischen IT und Datenschutz

Verbindung zwischen IT und Datenschutz

Technische und organisatorische Massnahmen (TOM)

Wirkungsvolle Sicherheitslösungen basieren auf einem ausbalancierten Zusammenspiel von **technischen** und **organisatorischen Massnahmen** (TOM). Nicht «entweder oder» ist das Rezept, sondern «sowohl als auch».

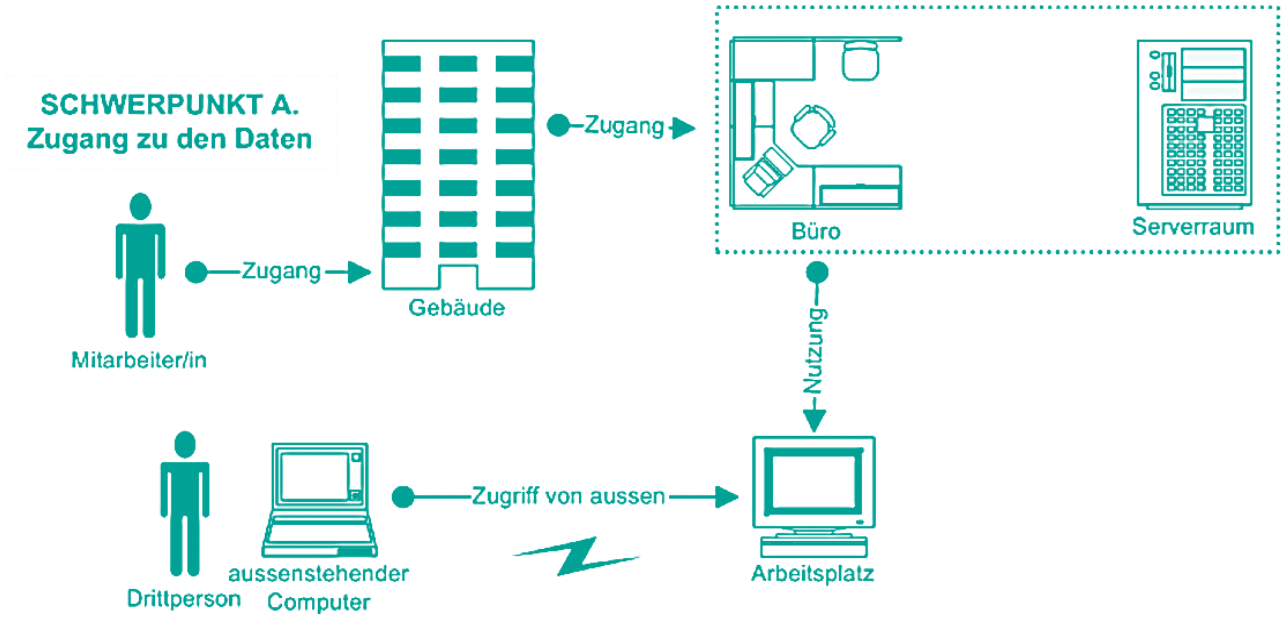
Ziel : Gewährleistung der Datensicherheit während des ganzen Lebenszyklus der Daten

Vier Schwerpunkte im Bezug auf TOM gemäss dem Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragten EDÖB

Zugang zu den Daten	Lebenszyklus von Daten	Datenaustausch	Auskunftsrecht
1. Sicherheit der Räumlichkeiten 2. Sicherheit der Serverräume 3. Sicherheit des Arbeitsplatzes 4. Identifizierung und Authentifizierung 5. Zugang zu den Daten 6. Zugang von Ausserhalb der Organisation	1. Datenerfassung 2. Protokollierung 3. Pseudonymisierung und Anonymisierung 4. Verschlüsselung 5. Sicherheit der Datenträger 6. Datensicherung 7. Datenvernichtung 8. Bearbeitung durch Dritte 9. Sicherheit und Schutz	1. Netzsicherheit 2. Verschlüsselung von Mitteilungen 3. Unterzeichnen von Mitteilungen 4. Übergabe von Datenträgern 5. Protokollierung des Datenaustauschs	1. Recht der betroffenen Personen 2. Reproduzierbarkeit der Verfahren

Verbindung zwischen IT und Datenschutz

Zugang zu den Daten



Quelle: Leitfaden zu den TOMs gemäss EDÖB

- Der Zugang zum Gebäude wird geregelt. Dank einem Badge und allenfalls einem Zugangscode können die Personen, die zugangsberechtigt sind, authentifiziert werden.
- Eine ähnliche Regelung wird nötig, wenn sich mehrere Organisationen im selben Gebäude befinden: Auf jeder Etage oder für jeden Gebäudeteil, der für eine bestimmte Organisation vorgesehen ist, wird eine elektronische Zugangskontrolle installiert.
- Für Besucherinnen und Besucher werden Zugang und Empfang so geregelt, dass sie sich nicht allein und frei im Gebäude bewegen können.
- Die Büros werden ausserhalb der Arbeitszeiten abgeschlossen.
- Es ist ratsam, in den heikelsten Räumen ein Alarmsystem zu installieren, das ausserhalb der Arbeitszeiten aktiviert wird.

Handlungsempfehlungen: Vorbereitung für den 1. September 2023

Handlungsempfehlungen für das Gesundheitswesen

Vorbereitung für den 1. September 2023

Das neue Schweizer Datenschutzgesetz sieht **keine relevanten Übergangsvorschriften** vor. Somit wird ein Grossteil der im Gesetz festgelegten Pflichten mit Inkrafttreten des nDSG **sofort** gelten. Es ist daher wichtig und wird empfohlen, sich frühzeitig vorzubereiten und bereits jetzt allfälligen Handlungsbedarf zu eruieren.

Vorbereitung

- **Verantwortlichkeiten klären**
- Ressourcen freistellen
- Interne/externe Unterstützung beziehen
- Prüfung der rechtlichen Bestimmungen

Ist-Analyse

- **nDSG analysieren und Know-how aufbauen**
- Prozesse analysieren
- Daten klassifizieren
- Richtlinien und DS-Erklärung studieren
- Lieferantenliste erstellen

Massnahmenplan

- Massnahmen festlegen
- Zeitliche und budgetäre Planung
- **Priorisierung der Ziele**
- Massnahmen umsetzen

Handlungsempfehlungen für das Gesundheitswesen

Vorbereitung für den 1. September 2023

1. Das Unternehmen intern so organisieren, dass klar ist wer Zugriff auf welche Daten hat und den Zugriff auf das Nötigste zu beschränken.

2. Einen schnellen und effektiven Prozessablauf für die Meldung von Datenschutzverletzungen festlegen.

3. Bestehende Datenschutzerklärungen sollten geprüft und angepasst werden. Falls noch keine Datenschutzerklärung vorliegt, sollte so rasch als möglich eine aufgesetzt werden.

4. Bereits bei der Entwicklung von neuen Technologien und Diensten sollte der Datenschutz miteinbezogen werden (Privacy by Design & Privacy by Default). Die Datenbearbeitung sollte wenn möglich auf ein Mindestmass reduziert werden.

5. Die Verträge mit Auftragsbearbeitern überprüfen, ob diese der kommenden Rechtslage entsprechen und allenfalls anpassen. Fall nötig Einwilligungen für eine Unter-Auftragsbearbeitung erteilen.

6. Datenschutzfolgenabschätzung erarbeiten und umsetzen.

7. Verzeichnis der Bearbeitungstätigkeiten erstellen.

8. Unternehmen sollten ihre Mitarbeitenden sensibilisieren und schulen.

Handlungsempfehlungen für das Gesundheitswesen

Vorbereitung für den 1. September 2023

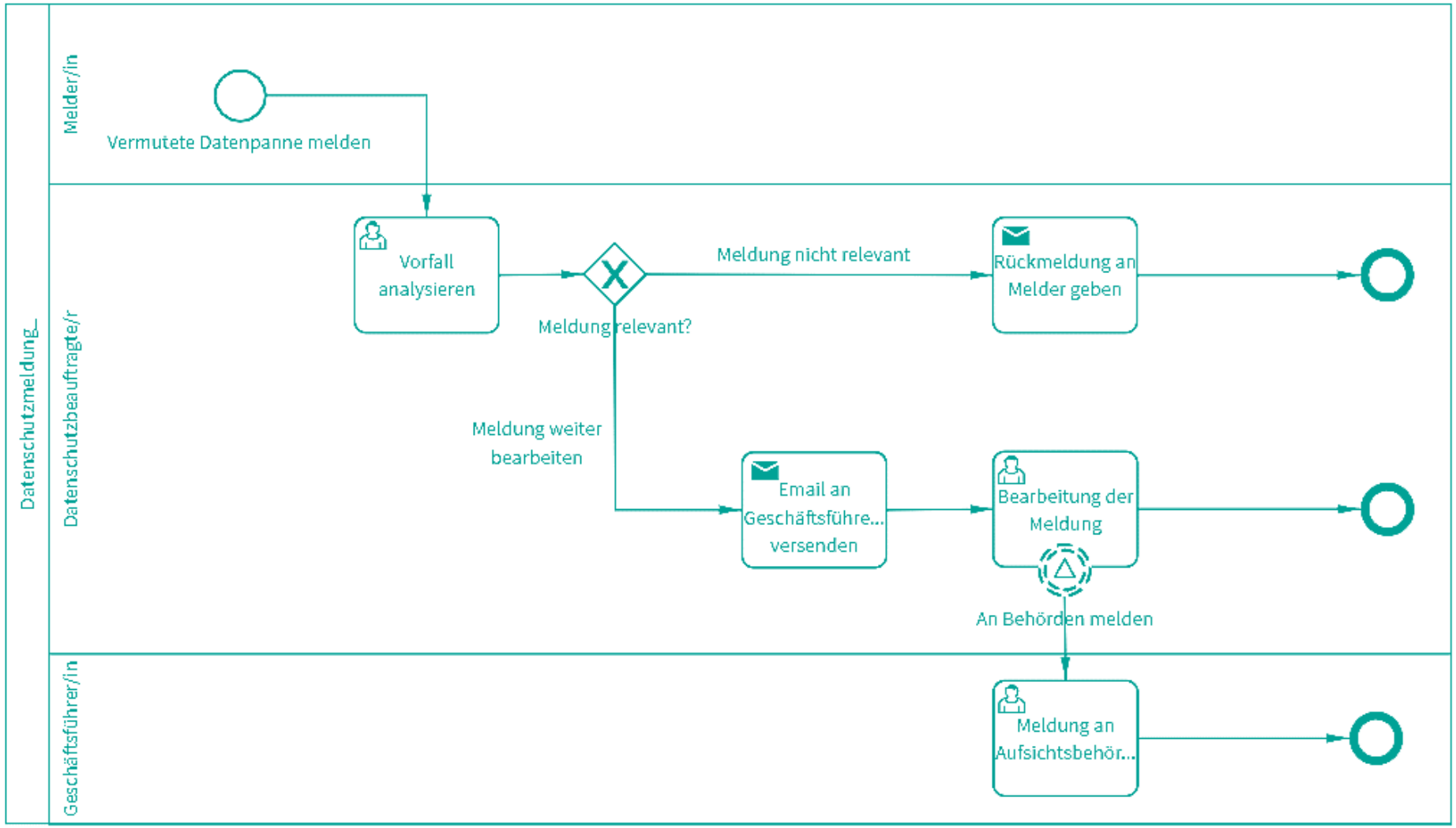
Hauptkategorie (Busine	Prozess	Applikation	Verantwortliche I	Bearbeitungstätigkeit	Bearbeitungszweck	Kategorien betr	Kategorien bearbeitete	Empfängerinnen	Werde	Aufbewahr	TOM
[COR] Hauptprozess	Dokumentenmanagement	[iManage] [Sharepoint] [andere] (zutreffendes auswählen)	[Anwaltskanzlei]	Erbringung und Dokumentation von Leistungen	Erbringung und Dokumentation von Leistungen	Mitarbeitende von Klientinnen, Gegenparteien, Behörden und Gerichten	Kontaktdaten, Beratungs- und Prozessführungsdaten, Rechnungsdaten	Intern, externe Dienstleister, Gegenparteien, Behörden und Gerichte	Nein	[10 Jahre] [Gemäss Aufbewahrungs-RL]	Gemäss Dokument TOM
[COR] Hauptprozess	Leistungserfassung	[iManage] [Sharepoint] [andere] (zutreffendes auswählen)	[Anwaltskanzlei]	Leistungserfassung	Leistungserfassung zwecks Abrechnung und Dokumentation	Klientinnen; Mitarbeitende von Klientinnen oder Gegenparteien	Kontaktdaten, Beratungs- und Prozessführungsdaten, Rechnungsdaten	Intern, Klientinnen, externe Dienstleister	Nein	[10 Jahre] [Gemäss Aufbewahrungs-RL]	Gemäss Dokument TOM
[ADM] Finanzen und Adminsitration	Rechnungswesen	[Vertec] [Bexio] [andere] (zutreffendes auswählen)	[Anwaltskanzlei]	Leistungsabrechnung	Abrechnung	Klientinnen; Mitarbeitende von Klientinnen oder Gegenparteien	Kontaktdaten, Beratungs- und Prozessführungsdaten, Rechnungsdaten	Intern, Klientinnen, externe Dienstleister	Nein	[10 Jahre] [Gemäss Aufbewahrungs-RL]	Gemäss Dokument TOM

Mindestinformationen

- Identität und Kontaktdaten des Verantwortlichen
- Bearbeitungszwecke
- Kategorien der Empfänger*innen (Auftragsbearbeiter oder Dritte als Verantwortliche)
- Kategorien bearbeiteter Personendaten
- Empfängerstaaten und Garantien bei Bekanntgabe ins Ausland

Handlungsempfehlungen

Vorbereitung für den 1. September 2023



Konsequenzen bei Nichtanwendung: Persönliche Strafbarkeit

Konsequenzen bei Nichtanwendung

Persönliche Strafbarkeit

- Die Art. 60-63 nDSG befassen sich primär mit Strafbestimmungen bei Verletzungen von Informations- und Auskunftspflichten.
- Eine Strafbarkeit für fahrlässige Verletzungen des nDSG ist nicht vorgesehen.
- Allerdings kann von einer vorsätzlichen Verletzung bereits dann ausgegangen werden, sobald die Verletzung in Kauf genommen wurde.

← Art. 60 → Verletzung von Informations-, Auskunfts- und Mitwirkungspflichten

1 Mit Busse bis zu 250 000 Franken werden private Personen auf Antrag bestraft:

a die ihre Pflichten nach den Artikeln 19, 21 und 25–27 verletzen, indem sie vorsätzlich eine falsche oder unvollständige Auskunft erteilen;

b die es vorsätzlich unterlassen:

1. die betroffene Person nach den Artikeln 19 Absatz 1 und 21 Absatz 1 zu informieren, oder
2. ihr die Angaben nach Artikel 19 Absatz 2 zu liefern.

2 Mit Busse bis zu 250 000 Franken werden private Personen bestraft, die unter Verstoss gegen Artikel 49 Absatz 3 dem EDÖB im Rahmen einer Untersuchung vorsätzlich falsche Auskünfte erteilen oder vorsätzlich die Mitwirkung verweigern.

Konsequenzen bei Nichtanwendung

Persönliche Strafbarkeit

Mit einer Busse von bis zu CHF 250'000 ist insbesondere Folgendes strafbar:

- Verletzung von Informationspflichten (z.B. keine oder nur eine ungenügende Datenschutzerklärung)
- Kein Vertrag mit Auftragsbearbeiter
- Verletzung der Datensicherheit (Verletzung der Vertraulichkeit, Verfügbarkeit oder Integrität der Daten, TOM)
- Bekanntgabe von Personendaten in Länder ohne ein angemessenes Datenschutzniveau, ohne das Treffen zusätzlicher Schutzmassnahmen oder ohne dass eine Ausnahme einschlägig ist (z.B. Einwilligung)
- Verletzung von Auskunftspflichten

Konsequenzen bei Nichtanwendung

Persönliche Strafbarkeit

Bei wem liegt die Zuständigkeit für die Strafverfolgung?

- Eine besondere Zuständigkeit für Verletzungen wird im nDSG nicht statuiert. Es sind die allgemeinen Strafverfolgungsbehörden der Kantone oder des Bundes zuständig.

- Gemäss Art. 65 Abs. 2 nDSG verfügt der EDÖB lediglich über ein Anzeigerecht. Die Möglichkeit als Privatklägerin im Strafverfahren aufzutreten, steht dem EDÖB jedoch offen. Das nDSG wurde eng an das StGB und die StPO angebunden.

- Die differenzierten Beschuldigtenrechte der StPO können somit von dem Beschuldigten wahrgenommen werden. Dem Staat steht dadurch wiederum die Möglichkeit offen, die durch die Verletzung des nDSG erzielten Vermögenswerte zu beschlagnahmen gem. Art. 70 StGB. Die Strafverfolgung unterliegt in diesen Fällen einer besonderen Verjährung gem. Art. 66 nDSG.

FAZIT

Fazit

Unsere Empfehlung für den Gesundheitssektor

Das nDSG ist kein technisches Projekt, sondern viel mehr ein organisatorisches.

- Klären Sie die Verantwortlichkeiten und planen genügende Ressourcen ein
- Machen Sie eine interne IST-Analyse Ihrer Prozesse und der darin bearbeiteten Daten
- Holen Sie sich externe Unterstützung
- **Schulen Sie Ihre Mitarbeitenden**

AVENIQ

Danke!