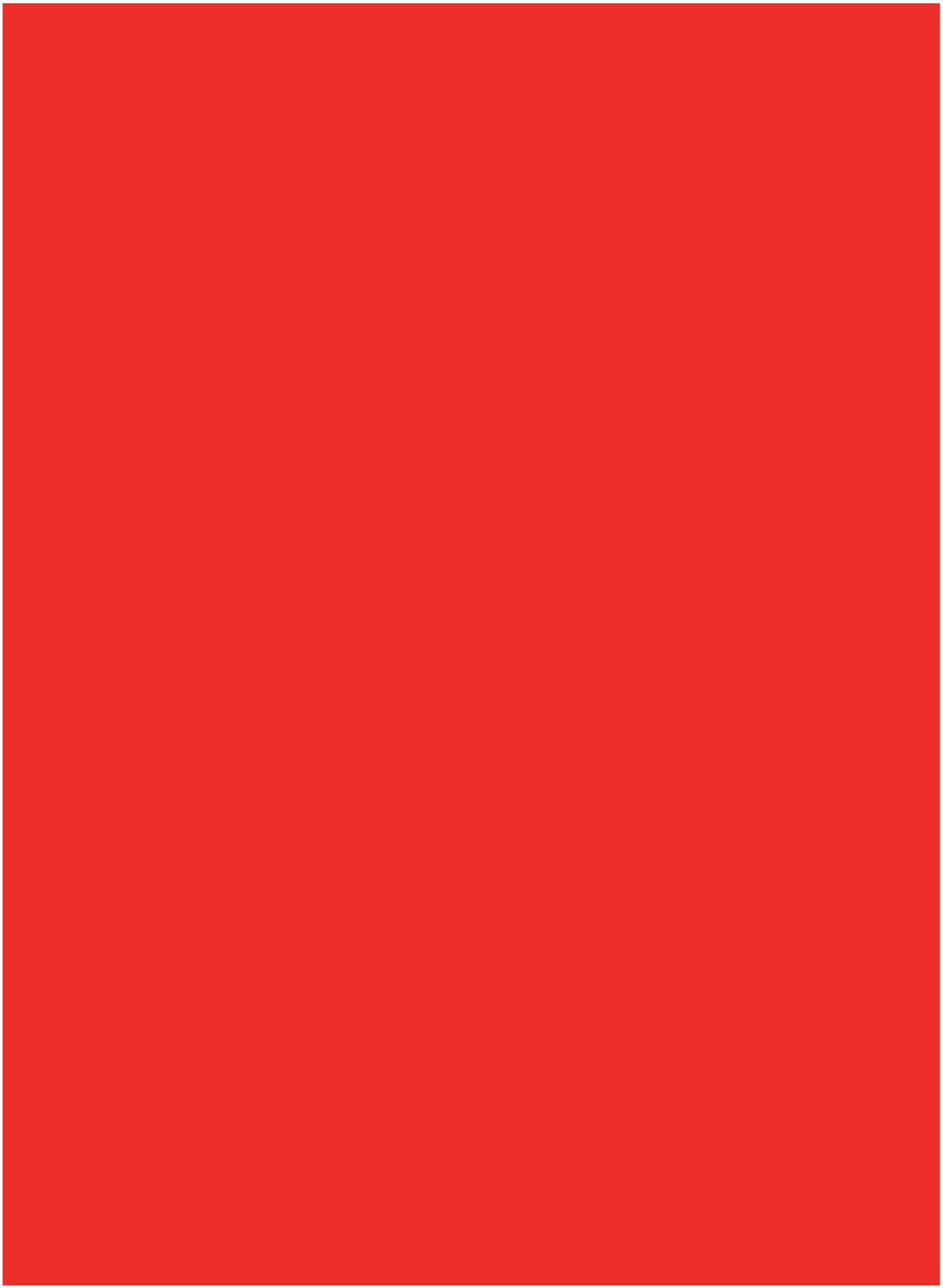
SWISS INSIGHTS

Swiss Data Insights Association

Swiss Insights News

#09

Datensicherheit



Datensicherheit: Herausforderungen und gesetzliche Pflichten

Marcel Griesinger
Rechtsanwalt,
Inhaber Rechtsanwaltskanzlei Griesinger, Hochschuldozent Wirtschafts- und Datenschutzrecht

Der nachfolgende Beitrag soll einen Überblick zu den gesetzlichen Anforderungen geben und zeigt an Beispielen konkrete Massnahmen im Bereich der Datensicherheit auf.

Sich häufende Cyberattacken haben das Thema der Datensicherheit in den Fokus gerückt. Gleichzeitig handelt es sich bei der Datensicherheit um eine Vorgabe, die das Datenschutzgesetz an die Unternehmen stellt.

Die Datensicherheit ist Bestandteil des Datenschutzrechts und damit auch des Datenschutzgesetzes. Im aktuell noch geltenden Datenschutzgesetz (DSG) ist die Datensicherheit in Art. 7 DSG geregelt. Danach müssen Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden. Per September 2023 wird das revidierte Datenschutzgesetz (revDSG) in der Schweiz in Kraft treten.
Die dann massgebliche Vorschrift zur Datensicherheit ist Art. 8 revDSG. Die Vorschrift formuliert in Absatz 1 die Anforderungen an die Datensicherheit wie folgt: «Der Verantwortliche und der Auftragsbearbeiter gewährleisten durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit.». Abs. 2 hält fest, dass die Massnahmen es ermöglichen müssen, Verletzungen der Datensicherheit zu vermeiden. Darüber hinaus bestimmt Abs. 3, dass der Bundesrat Bestimmungen über die Mindestanforderungen an die Datensicherheit erlässt.
Dies erfolgt konkret mittels der Verordnung zum Datenschutzgesetz (VDSG). Die Revision des DSG erfordert eine Anpassung der VDSG. Davon sind auch die Regelungen über die Mindestanforderungen an die Datensicherheit betroffen. Die VDSG befindet sich daher aktuell in der Revision, es ist bisher ein Entwurf (E-VDSG) veröffentlicht und in die (nunmehr bereits abgeschlossene) Vernehmlassung geschickt worden.
Im Rahmen der Vernehmlassung äusserten Anwender wie Verbände, Kanzleien und Unternehmen erhebliche Kritik am E-VDSG. Insbesondere kritisierten sie, dass der bisherige Entwurf zu detaillierte und zu umfangreiche Vorgaben für Unternehmen, insbesondere für KMU, enthalte. Im Hinblick auf hier noch zu erwartende Ergänzungen und/oder Anpassungen durch den Gesetzgeber bleibt abzuwarten, welches Anforderungsniveau und welche konkreten Massnahmen zur Datensicherheit die revidierte VDSG (revVDSG) an Unternehmen stellt. Die aktuelle Entwicklung hierzu sollten die Fachverantwortlichen im Unternehmen genau beobachten.

Vorgaben an die Datensicherheit nach dem aktuellen DSG

Zentrale Vorgabe der gesetzlichen Regelung ist es, Personendaten gegen die unbefugte Bearbeitung zu schützen. Dabei hat der Schutz der Daten vor den Risiken einer unbefugten Bearbeitung durch angemessene organisatorische und technische Massnahmen zu erfolgen. Üblicherweise erfolgt eine Analyse potentieller Risiken und erforderlicher Massnahmen im Rahmen eines Datensicherheitskonzepts. Dieses ermöglicht eine gesamtheitliche Bewertung

und Einordnung der ergriffenen Massnahmen. In der VDSG sind verschiedene technische und organisatorische Massnahmen umschrieben. Zu beachten sind insbesondere die Art. 8 bis 11 VDSG sowie die Art. 20 und 21 VDSG (für Bundesorgane).

Bereits erkennbare Vorgaben aus der Botschaft zum revDSG

In den Gesetzgebungsmaterialien zum revDSG sind grundsätzliche Überlegungen zu den Anforderungen an die Datensicherheit enthalten. Die Vorschrift des Art. 8 revDSG geht von einem risikobasierten Ansatz aus. Die Botschaft (Botschaft Totalrevision Datenschutzgesetz BBl 2017 7031) formuliert hierzu «Je grösser das Risiko einer Verletzung der Datensicherheit, umso höher sind die Anforderungen an die zu treffenden Massnahmen.» Darüber hält die Botschaft fest, dass sowohl Verantwortliche als auch Auftragsbearbeiter dazu verpflichtet sind, «für ihre Systeme eine geeignete Sicherheitsarchitektur vorzusehen und sie z. B. gegen Schadsoftware oder Datenverlust zu schützen».

Bereits jetzt empfohlene, ausgewählte Massnahmen zur Daten- und Cybersicherheit

Bereits jetzt empfehlen sich verschiedene Massnahmen zur Datensicherheit. Dabei kommen sowohl technische als auch organisatorische Massnahmen in Betracht, welche das Risiko eines erfolgreichen Cyberangriffs mindern. Nachfolgend werden einzelne, ausgewählte Massnahmen vorgeschlagen. Es ist zu beachten, dass es sich dabei nicht um eine abschliessende oder vollumfängliche Aufzählung aller potentiellen oder relevanten Massnahmen handelt.

Schulung und Sensibilisierung von Mitarbeitenden

Eine wesentliche organisatorische Massnahme stellt die hinreichende Schulung und Sensibilisierung der Mitarbeitenden dar. Der menschliche Faktor ist in einer Sicherheitsarchitektur häufig eine Schwachstelle. Der unzureichende Schutz von Zugangscodes, Passwörtern, Zugangsberechtigungen, usw. stellt ein potentielles Einfallstor für unbefugte Zugriffe dar. Entsprechende Schulung der Mitarbeitenden kann ein erhebliches Mass an Awareness für Risikosituationen und das richtige Verhalten schaffen.

Zugriffsberechtigungen

Wenn unternehmensintern über alle Stufen und Abteilungen hinweg weitgehende Zugriffsrechte auf sämtliche Informationen und Daten bestehen, wird dies häufig mit flachen Hierarchien und schnellen Entscheidungswegen gerechtfertigt. Unter dem Aspekt der Datensicherheit müssen indessen tatsächlich nur sehr wenige Mitarbeitende derart weitreichende Zugriffsrechte haben. Um Daten auch intern vor nicht erforderlichen Zugriffen und damit potentiellen Risiken zu schützen, wird empfohlen nur diejenigen Zugriffsrechte zu gewähren, die der Mitarbeitende für seine Tätigkeit auch tatsächlich benötigt. Zur Vermeidung der (unbeabsichtigten) Installation von Schadsoftware ist in diesem Zusammenhang überdies zu empfehlen, dass die Berechtigung zur Installation von Software nur sehr eingeschränkt vergeben wird und stattdessen den Mitarbeitenden ein verstärkter IT-Support zur Verfügung steht.

Aktualität der eingesetzten IT-Anwendungen

Schadsoftware nutzt häufig Lücken in veralteten Softwareanwendungen aus. Daher wird empfohlen die Betriebssysteme stets mit den aktuellen Updates/Sicherheitsupdates auf den neusten Stand zu bringen. Zugleich sind auch Browser und sonstige Softwareanwendungen im Hinblick auf die Aktualität ihrer Updates zu prüfen. Zudem sollten alle im Einsatz befindlichen Geräte, also nicht nur Laptops, sondern auch Mobiltelefone, Drucker, Tablets, usw. daraufhin kontrolliert werden, ob ihre Betriebssysteme und Sicherheitsupdates auf dem neusten Stand sind. Auch wenn Mitarbeitende eigene Geräte nutzen (BYOD), ist auf die Aktualität der Schutzmassnahmen zu achten. Schliesslich

gilt es entsprechende Schutzsoftware (sog. Virenschutz) vorzuhalten und Firewalls zum Schutz des eigenen Systems zu aktivieren.

Verschlüsselung

Bei der Bearbeitung von wichtigen und/oder sensiblen Daten ist stets darauf zu achten, dass diese nur verschlüsselt gespeichert, übermittelt oder transportiert werden.

Vertragsmanagement

Im Zusammenhang mit der Bearbeitung und Auslagerung von Datenbearbeitungsvorgängen, beispielsweise indem Cloud-Dienstleister, (Online-)CRMs, Analyse-Tools usw., zum Einsatz kommen, ist stets die Frage nach der Wahrung der Sicherheit für die betroffenen Datensätze zu beachten. Hier kommen insbesondere vertragsrechtliche Regelungen mit der anderen Partei in Betracht. Diese regeln die einzuhaltenden Standards, beinhalten klare Vorgehensweisen bei Verstössen gegen die Datensicherheit, bestimmen Meldepflichten an den Vertragspartner und benennen Haftungsregeln, Verantwortungssphären usw. Darüber hinaus können Unternehmen vom Vertragspartner auch verlangen, dass er ein Sicherheitskonzept vorlegt. Wie die Einhaltung der vereinbarten Sicherheitsstandards kontrolliert wird oder werden kann, ist üblicherweise Teil des Vertrags zwischen dem Unternehmen und dem Partner, welcher Daten extern bearbeitet.

Weitere zusätzliche Regelungsinhalte werden dann erforderlich, wenn es sich um einen ausländischen Vertragspartner handelt. Hat dieser seinen Sitz darüber hinaus in einem Land, das kein gleichwertiges Datenschutzniveau bietet (vgl. hierzu die Länderliste des EDÖB), werden weitere vertragliche (u. a. Verwendung von Standardvertragsklauseln) und prozessuale (DTIAs = Data Transfer Impact Assessments; Risikoabschätzung hinsichtlich der geplanten Datentransfers) Massnahmen erforderlich, um die Datensicherheit hinreichend zu gewährleisten. Dies ist insbesondere im Fall von Datentransfer in die USA, bspw. bei Nutzung von US-Cloud-Dienstleistungen, Online-CRMs, usw., erforderlich.

Empfehlung

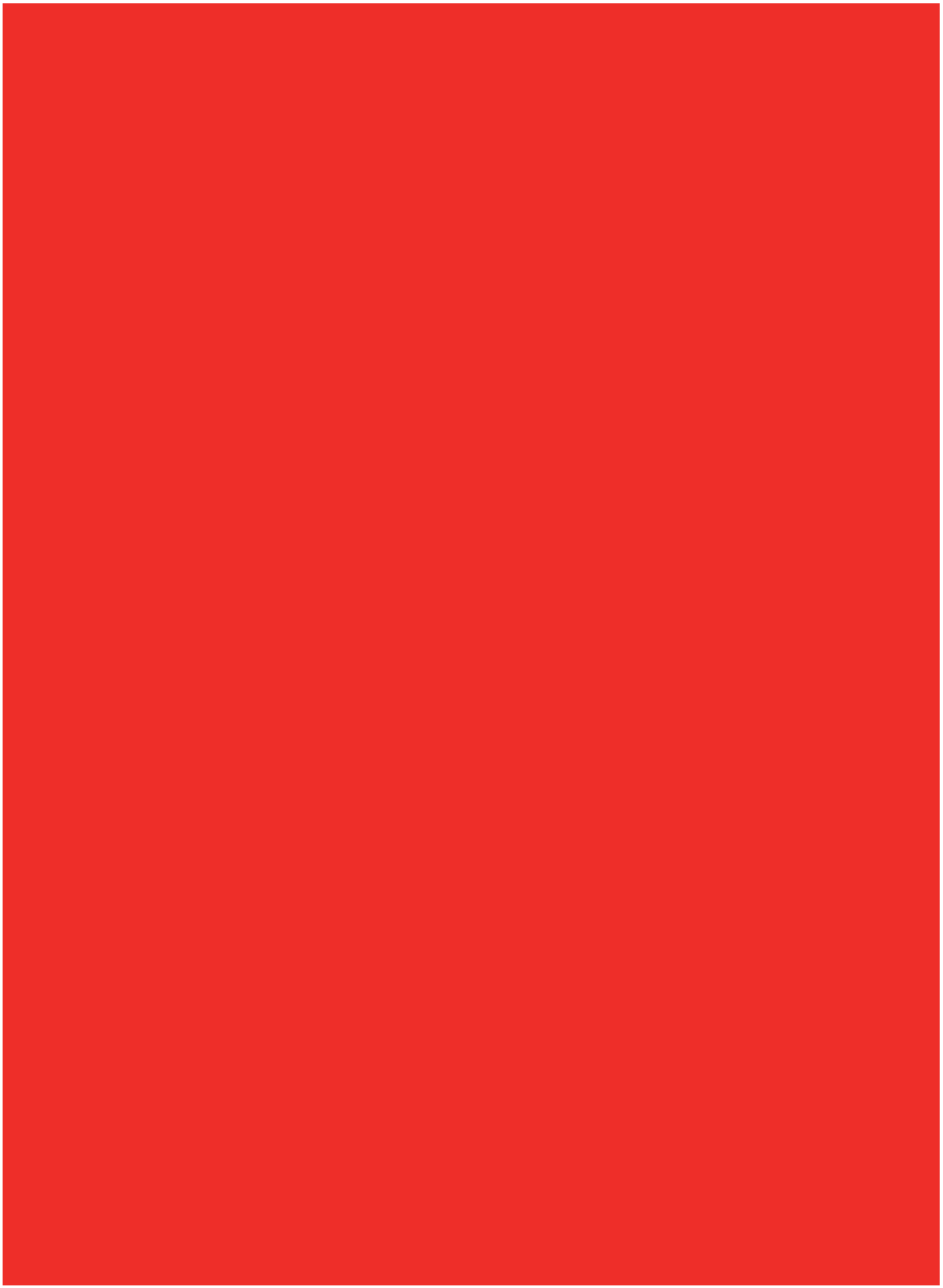
Die Datensicherheit ist eine zentrale datenschutzrechtliche Vorgabe, die im DSG wie auch dem revDSG festgehalten ist. Zur Umsetzung der Datensicherheit im Unternehmen empfiehlt es sich ein Sicherheitskonzept zu erstellen, das den rechtlichen Anforderungen entspricht und diese technisch umsetzt. Darüber hinaus kommt der vertraglichen Ausgestaltung zur Datensicherheit bei Datentransfers eine besondere Bedeutung zu. Hinsichtlich der neuen und konkretisierten Anforderungen an die Datensicherheit durch die revVDSG bleibt der Umfang der umzusetzenden Massnahmen abzuwarten. Diese Massnahmen lassen sich je nach Ausmass der Anforderungen indessen in ein bestehendes Sicherheitskonzept integrieren, so dass sich dessen Erstellung schon jetzt anbietet.

Der Autor

Marcel Griesinger, Rechtsanwalt, Inhaber Rechtsanwaltskanzlei Griesinger, die auf Business Law und Corporate Privacy Law spezialisiert ist, Hochschuldozent Wirtschafts- und Datenschutzrecht

Kontakt

Rechtsanwaltskanzlei Griesinger, Marcel Griesinger
marcel.griesinger@kanzlei-griesinger.ch
+41 79 871 52 56



Swiss Insights

Swiss Insights ist der Verband und die Interessensvertretung aller Unternehmen, die Daten und prädiktive Modelle im Rahmen von Marketing, Innovationsprozessen, Kundenservice, Angebotsgestaltung, Kommunikation und Zielgruppendefinitionen erheben, analysieren, einsetzen und daraus Handlungsempfehlungen ableiten.

Swiss Insights pflegt einen aktiven Dialog mit politisch und gesellschaftlich wichtigen Akteuren und fördert den Austausch mit anderen nationalen und internationalen Fachorganisationen.

Eine der Hauptaufgaben des Verbands ist die Förderung der Markt-, Meinungs- und Sozialforschung im Allgemeinen und der Wissenschaftlichkeit im Besonderen. Er entwickelt, definiert und unterhält strenge Leitlinien zur Qualitätssicherung und grenzt sich im Bereich der Markt- und Sozialforschung klar von Werbung und Direktmarketing ab. Hierzu führt der Verband das Qualitätslabel «Market & Social Research by Swiss Insights».

Darüber hinaus engagiert sich Swiss Insights dafür, dass die Nutzung von Daten und die Anwendung von datengetriebenen Modellen transparent, nachvollziehbar und in diesem Sinne fair gestaltet wird. Hierfür wurde das Label «Data Fairness by Swiss Insights» geschaffen.

Herausgeber und Kontakt
Swiss Insights, Swiss Data Insights Association, Gruebengasse 10, 6055 Alpnach, Switzerland
+41 44 3501960, info@swiss-insights.ch, www.swiss-insights.ch

Unsere Mitglieder

SWISS INSIGHTS Institute Member

Im Verband sind alle relevanten **Markt- und Sozialforschungsinstitute** unter einem Dach organisiert. Alle Mitgliedsinstitute unterliegen einem strengen Regelwerk von schweizerischen und internationalen Normen.

Mitgliedsinstitute dürfen das Label **Market & Social Research by SWISS INSIGHTS** und je nach Tätgikeitsgebiet das Label **Data Fairness by SWISS INSIGHTS** tragen.

Die Mitgliederliste finden Sie auf der nachfolgenden Seite.

SWISS INSIGHTS Corporate Member

Die Corporate Mitglieder sind **Unternehmen**, die sich für den fairen Umgang mit Auskunftspersonen und Auftraggeber sowie für den Schutz der Privatsphäre engagieren.

Corporate Member, die das Label **Data Fairness by SWISS INSIGHTS** tragen, stehen für den wissenschaftlichen, seriösen und respektvollen Umgang mit Daten ein.

Die Mitgliederliste finden Sie auf der nachfolgenden Seite.

SWISS INSIGHTS

Institute Member

amPuls Market Research
Hirschengraben 49, 6000 Luzern 7
+41 41 612 14 14 / info@ampuls.ch
www.ampuls.ch

amrein+heller MarktforschungsTreuhand AG
Südweid 7, 6274 Eschenbach
+41 748 63 70 / contact@ah-feedback.ch
www.ah-feedback.ch

Bilendi Schweiz AG
Reinhardstrasse 19, 8008 Zürich
+41 79 801 88 80 / contact.ch@bilendi.com
www.bilendi.ch

Boomerang Ideas AG
Sihlquai 131, 8005 Zürich
+41 44 500 88 60 / raphael@boomerangideas.com
www.boomerangideas.com

Constant Dialog
Alte Steinhauserstrasse 33, 6330 Cham
+41 41 310 05 40 / info@constant-dialog.ch
www.constant-dialog.ch

DemoSCOPE Data + Research
Klusenstrasse 17, 6043 Adligenswil
+41 41 375 40 00 / demoscope@demoscope.ch
www.demoscope.ch

dr-ouwerkerk ag – just-medical!
Blegistrasse 5, 6340 Baar
+41 41 766 11 55 / info@just-medical.com
www.pharmaagentur.ch

Gallup AG
Reinhardstrasse 19, 8008 Zürich,
+41 78 891 31 15 / office@gallup.swiss
www.gallup.swiss

gff Swiss Research Services
Baarerstrasse 25, 6300 Zug
+41 41 560 01 60 / gut@gff.ag,
www.gff.ag

GfK Switzerland AG
Suurstoffi 18A, 6343 Rotkreuz
+41 41 632 91 11 / info.ch@gfk.com
www.gfk.ch / www.gfk.com

gfs.bern. Menschen. Meinungen. Märkte.
Effingerstrasse 14, Postfach, 3001 Bern
+41 31 311 08 06 / info@gfsbern.ch
www.gfsbern.ch

gfs-zürich, Markt- & Sozialforschung
Riedtlistrasse 9, 8006 Zürich
+41 44 360 40 20 / gfs@gfs-zh.ch
www.gfs-zh.ch

gfs-befragungsdienst
Schaffhauserstrasse 491, 8052 Zürich
+41 44 360 26 40 / info@gfs-bd.ch
www.gfs-bd.ch

GIM Suisse AG
General-Wille-Strasse 10, 8002 Zürich
+41 44 283 18 18 / info@g-i-m.ch
www.g-i-m.ch

Happy Thinking People AG
Staufacherstrasse 101, 8048 Zürich
+41 44 204 16 26 / contact-zurich@happythinkingpeople.com
www.happythinkingpeople.com

INNOFACT (Schweiz) AG Research & Consulting
Flurstrasse 50, 8048 Zürich
+41 43 931 77 82, Info@innofact.ch
www.innofact.ch

Instight Institute AG
Bergstrasse 138, 8032 Zürich
+41 44 387 90 90 / info@insightinstitute.ch
www.insightinstitute.ch

intervista
Optingenstrasse 5, 3013 Bern
+41 31 511 39 00 / anfragen@intervista.ch
www.intervista.ch

IPSOS Suisse SA
11, Chemin du Château-Bloch, 1219 Le Lignon
+41 22 591 06 00 / Contact_Switzerland@ipsos.com
www.ipsos.com/de-ch

Kantar Media Switzerland AG
Bahnhofstrasse 4, 3073 Gümligen
+41 31 537 79 00 / ch.panel@kantarmedia.com
www.kantarmedia.com

SWISS INSIGHTS
Institute Member

LINK
Baslerstrasse 60, 8048 Zürich
+41 41 367 73 73 / zurich@link.ch
www.link.ch

Marketagent.com Schweiz AG
Seefeldstrasse 19, 8008 Zürich
+41 43 555 06 50, schweiz@marketagent.com
www.marketagent.com

M.I.S. Trend SA
Pont Bessières 3, 1005 Lausanne
+41 21 320 95 03 / info@mistrend.ch
www.mistrend.ch

onlineumfragen.com GmbH
Kernserstrasse 15, 6056 Kägiswil
+41 44 500 50 54 / info@onlineumfragen.com
www.onlineumfragen.com

POLYQUEST AG
Flurstrasse 26, 3014 Bern
+41 31 335 64 00 / info@polyquest.ch
www.polyquest.ch

Publicom AG
Alte Landstrasse 55, 8802 Kilchberg
+41 44 716 55 11 / publicom@publicom.ch
www.publicom.ch

Qualitest AG, Institut für Marketing- und Sozialforschung
Rosenberghöhe 3, 6004 Luzernr
+41 41 712 12 21 / qualitest@qualitestag.ch
www.qualitestag.ch

SensoPLUS
Industriestrasse 16, 6300 Zug
+41 41 710 71 61 / info@sensoplus.ch
www.sensoplus.ch

NielsenIQ (Switzerland) GmbH
Park 4, 6039 Root D4
+41 41 445 64 64 / nielsen-ch@nielsen.com
www.nielsen.com

TransferPlus AG Market Research
Haldenstrasse 11, 6006 Luzern
+41 41 618 33 11 / transfer@transferplus.ch
www.transferplus.ch

SWISS INSIGHTS
Corporate Member

BSI Business Systems Integration AG
Täfernweg 1, 5405 Baden
+41 58 255 90 00, info@bsi-software.com
www.bsi-software.com