Das neue Schweizer Datenschutzrecht

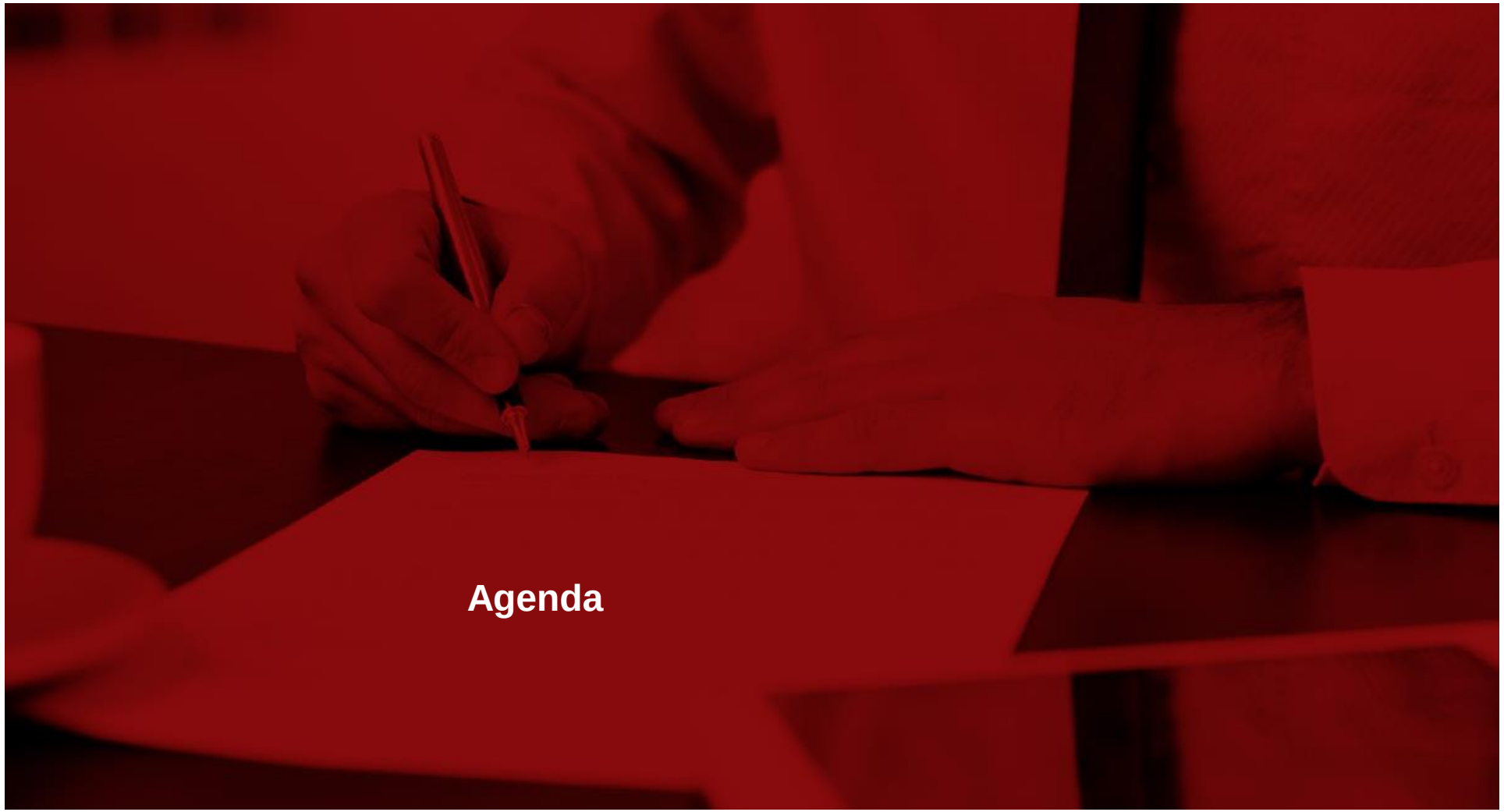
Was bedeutet dies für die Treuhandbranche? Was bedeutet dies in Bezug auf unsere Arbeit?

ROESLE FRICK & PARTNERS

EXPERTsuisse
Sektion Zentralschweiz – 24. Mai 2023

Die Gretchen-Frage? Wie haben Sie es in Ihrem Unternehmen mit dem Datenschutz?

- Wir haben bereits die EU DSGVO sowie das neue DSG umgesetzt?
- Wir haben die EU DSGVO umgesetzt und deshalb müssen wir für das neue DSG nichts Weiteres vorkehren?
- Wir haben das neue DSG bereits umgesetzt?
- Wir haben mit der Umsetzung des neuen DSG begonnen?
- Wir starten die Umsetzung des neuen DSG mit der heutigen Veranstaltung?
- Wir werden das noch umsetzen.


Agenda

Eine Tour d'Horizon über das neue DSG

1. Das revidierte Datenschutzgesetz
2. Was ändert sich mit dem revidierten Datenschutzgesetz?
3. Wie setzen Sie diese Änderungen in Ihrem Unternehmen um?
4. Was bedeutet dies für die Treuhandbranche?
5. Was bedeutet dies in Bezug auf unsere Arbeit?
6. Haben Sie noch Fragen oder Anmerkungen?

Das revidierte Datenschutzgesetz

ROESLE FRICK & PARTNERS

Das revidierte bzw. neue Datenschutzgesetz

- Angleichung des Schweizer Rechts an das EU-Recht
  -> Beibehaltung prinzipienbasierter Regelungen gemäss dem bisherigen Schweizer Recht
- Einführung neuer Pflichten für Unternehmen
- Notwendigkeit vermehrter Dokumentation
- Es wird kein Konzernprivileg geben
- Jeder Datenverarbeiter in der Schweiz fällt in den Anwendungsbereich des revDSG
  -> Datenschutz wird für jedes Unternehmen relevant
- Die Zeit läuft, da das Gesetz keine Übergangsfrist kennt
- Der zahnlose Tiger soll durch die Einführung von Sanktionen Biss bekommen

ROESLE FRICK & PARTNERS

Was ändert sich am 1. September 2023?

Thema	aDSG	revDSG
Zweck und Geltungsbereich	Anwendung auf natürliche und juristische Personen	Anwendung auf natürliche Personen und neu Definition des geografischen Anwendungsbereichs
Grundsätze	im Wesentlichen identisch	
Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen	n/a	neu
Datensicherheit	im Wesentlichen identisch	
Auftragsbearbeitung	vorhanden	erweitert hinsichtlich Pflicht zur Sicherstellung Datenschutz
Datenschutzberater	vorhanden	erweiterte Rolle
Bearbeitungsverzeichnis	n/a	neu
Schweizer Vertretung	n/a	neu
Bekanntgabe ins Ausland	im Wesentlichen identisch	
Informationspflichten	vorhanden	erweitert
Automatisierte Einzelentscheidungen	n/a	neu
Datenschutz-Folgenabschätzung	n/a	neu
Meldung von Datenschutzverletzungen	n/a	neu
Betroffenenrechte	vorhanden	leicht angepasst
Kompetenzen des EDÖB	eingeschränkt vorhanden	erheblich erweitert
Sanktionen	eingeschränkt vorhanden	erheblich erweitert
Dokumentationserfordernisse	eingeschränkt vorhanden	erheblich erweitert

Zwecke und Geltungsbereich

Was sagt das Recht?

- Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, über die Personendaten bearbeitet werden
- Persönlicher und sachlicher Geltungsbereich
  - Kundendaten sind i.d.R. Personendaten
- Erweiterter geografischer Anwendungsbereich («Auswirkungsprinzip»)

Was bedeutet dies in der Praxis?

-> Unternehmen müssen Datenschutz gegenüber ihren Mitarbeitern, Kunden und weiteren Dritten umsetzen

-> Unternehmen müssen Datenschutzverständnis schaffen

-> Unternehmen sollten Ihre ausländischen Kunden, welche eine Geschäftstätigkeit in der Schweiz ausüben auf die Anwendbarkeit des DSG hinweisen

Datenschutz Grundsätze

Was sagt das Recht?

- Rechtmässigkeit
- Treu und Glauben
- Verhältnismässigkeit
- Zweckgebundenheit und Erkennbarkeit /Transparenz
- Dauer (Datensparsamkeit)
- Richtigkeit

Was bedeutet dies in der Praxis?

-> Unternehmen müssen sich bewusst werden, welche Daten im Unternehmen bearbeitet werden

-> Unternehmen müssen Ihre Tätigkeit hinsichtlich der Einhaltung der Grundsätze prüfen

-> Unternehmen müssen ihre Mitarbeiter schulen und Datenschutzverständnis schaffen

Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

Was sagt das Recht?

- Datenbearbeitungen sind technisch und organisatorisch so auszugestalten, dass die Datenschutzvorschriften eingehalten werden
- Anforderungen Massnahmen
  - Stand der Technik
  - der Art und dem Umfang der Datenbearbeitung sowie dem Risiko angemessen
- Voreinstellungen zur Sicherstellung, dass die Bearbeitung der Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt ist

Was bedeutet dies in der Praxis?

-> Die Umsetzung dieser Anforderung kann einen Einfluss auf eine allfällige Cyberrisikoversicherung haben

-> Möglich Massnahmen;

-> Cookie-Banner auf der Webseite

-> Erarbeiten von Aufbewahrungsgrundsätzen

-> Zugangsschranken

-> Mitarbeiterschulungen

DATENSICHERHEIT

Was sagt das Recht?

- Dem Risiko angemessene Datensicherheit
- Massnahmen sollen Datensicherheitsverletzungen vermeiden
- Mindestanforderungen:
  - Im Hinblick auf das Risiko geeignete technische und organisatorische Massnahmen
  - Berücksichtigung des Stands der Technik und der Implementierungskosten

Was bedeutet dies in der Praxis?

-> Nichteinhaltung kann strafrechtliche Sanktionen nach sich ziehen

-> Umsetzung kann «Business Continuity» sicherstellen

-> Umsetzung kann mögliche Haftung im Falle einer Datensicherheitsverletzung minimieren

-> Umsetzung kann Reputationsschaden minimieren

AUFTRAGSBEARBEITUNG

Was sagt das Recht?

- Bearbeitung kann durch Vertrag oder durch Gesetz an einen Dritten übertrag werden, sofern dieser
  - Datenschutzniveau sichergestellt
  - Keine gesetzliche oder vertragliche Pflicht, welche die Übertragung verbietet
- Vergewisserungspflicht hinsichtlich Datensicherheit
- Vorgängige Genehmigung zur Übertragung notwendig
  - Die Genehmigung kann allgemeiner Natur oder spezifischer Art sein
  - Bei einer allgemeinen Einwilligung, hat der Verantwortliche über jede Veränderung der Dritten zu informieren

Was bedeutet dies in der Praxis?

-> Nichteinhaltung kann strafrechtliche Sanktionen nach sich ziehen

-> Abschluss Auftragsbearbeitungsvertrag

-> Anpassung bestehender Verträge insbesondere der AGB (z.B. Genehmigung von Datenbearbeitern)

-> Über Veränderungen von Dritten (z.B. Software-Anbieter) muss bei einer allgemeinen Einwilligung jedes Mal informiert werden

DATENSCHUTZBERATER

Was sagt das Recht?

- Private Verantwortliche **können** eine Datenschutzberaterin oder einen Datenschutzberater ernennen
- Bei Ernennung kann der private Verantwortliche von der Konsultation des EDÖB bei einer Datenschutz-Folgenabschätzung absehen

Was bedeutet dies in der Praxis?

-> Es ist nicht zwingend, dass ein Unternehmen einen Datenschutzbeauftragten bestellt

-> Wenn ein Datenschutzbeauftragter bestellt wird, ist bzw. sind diesem…

- … die notwendigen Ressourcen zur Verfügung zu stellen
- … Zugang zu allen Auskünften, Unterlagen, Verzeichnissen und Personendaten zu gewähren
- … die Berechtigung in wichtigen Fällen das oberste Leitungs- oder Verwaltungsorgan zu informieren einzuräumen

-> Ungeachtet dessen sollte in jedem Unternehmen ein interner Datenschutz-Champion bzw. eine klare Ansprechperson bezeichnet werden

BEARBEITUNGSVERZEICHNIS

Was sagt das Recht?

- Es ist ein Verzeichnis über die Bearbeitungstätigkeit zu führen
- Ausnahme:
  - Unternehmen mit weniger als 250 Mitarbeiter: oder
  - natürliche Personen, wenn keine besonders schützenswerte Personendaten in grossem Umfang bearbeitet werden oder Profiling mit hohem Risiko durchgeführt wird
- Mindestinhalt des Verzeichnis:
  - Identität des Verantwortlichen (und des Auftragsverarbeiters)
  - Bearbeitungszweck
  - Beschreibung der Kategorien betroffener Personen und bearbeiteter Personendaten
  - Kategorien von Empfängern
  - Aufbewahrungsdauer oder Kriterien zur Festlegung der Dauer
  - Beschreibung Massnahmen zur Gewährleistung der Datensicherheit soweit möglich
  - Bei Auslandsbekanntgabe, der Staat sowie die Garantien

Was bedeutet dies in der Praxis?

-> Viele werden gemäss Schweizer Datenschutzrecht kein Bearbeitungsverzeichnis führen müssen

-> ABER:

- Die DSGVO kennt keine Ausnahmebestimmung
- Um das revDSG sorgfältig umzusetzen, bedarf es einer Übersicht der Datenbearbeitungen

Schweizer Vertretung

Was sagt das Recht?

- Private Verantwortliche mit Sitz oder Wohnsitz im Ausland müssen eine Vertretung in der Schweiz bezeichnen
- Voraussetzungen:
  - Bearbeiten von Personendaten von Personen in der Schweiz
  - Die Bearbeitung steht im Zusammenhang mit dem Angebot von Waren und Dienstleistungen oder der Beobachtung des Verhaltens von Personen in der Schweiz
  - Umfangreiche Bearbeitung
  - Regelmässige Bearbeitung
  - Die Bearbeitung bringt ein hohes Risiko für die Persönlichkeit der betroffenen Personen mit sich
- Vertreter führt ein Verzeichnis der Bearbeitungstätigkeiten

Was bedeutet dies in der Praxis?

-> Machen Sie Ihre ausländischen Kunden auf diese Pflicht aufmerksam

Bekanntgabe ins Ausland

Was sagt das Recht?

- Bekanntgabe ins Ausland, wenn
  - ein angemessenes Datenschutzniveau vom Bundesrat anerkannt ist
  - ein völkerrechtlicher Vertrag besteht, der einen geeigneten Datenschutz gewährleistet
  - vom EDÖB anerkannte Datenschutzklauseln oder Standarddatenschutzklauseln(z.B. SCC) vereinbart wurden
  - verbindliche unternehmensinterne vom EDÖB genehmigte Datenschutzvorschriften einen angemessenen Schutz gewährleisten
  - im Einzelfall die betroffene Person ausdrücklich ihre Einwilligungen gegeben hat
  - die Bekanntgabe in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags zwischen Verantwortlichen und der betroffenen Person steht oder vom Verantwortlichen im Interesse der betroffenen Person geschlossen wird
- Veröffentlichung von Personendaten insbesondere über das Internet zur Information der Öffentlichkeit ist keine Bekanntgabe ins Ausland

Was bedeutet dies in der Praxis?

-> Nichteinhaltung kann strafrechtliche Sanktionen nach sich ziehen

-> Sofern keine Anerkennung des Bundesrats besteht, ist in der Regel mit Standardvertragsklauseln zu arbeiten

-> Bekanntgabe an eine Konzerngesellschaft im Ausland ist auch eine Bekanntgabe ins Ausland

INFORMATIONSPFLICHTEN

Was sagt das Recht?

- Der Verantwortliche muss angemessen informieren
- Mindestinhalt:
  - Identität und Kontaktdaten des Verantwortlichen
  - Bearbeitungszweck
  - Empfänger oder Kategorien von Empfängern denen Personendaten bekanntgegeben werden
  - Kategorien der bearbeiteten Personendaten (falls nicht direkt bei der betroffenen Person beschafft)
  - Bei Bekanntgabe ins Ausland, den Staat und gegebenenfalls die Garantien für die Bekanntgabe
- Es gibt Ausnahmen und Einschränkungen der Informationspflicht, z.B.:
  - Betroffene Person verfügt bereits über die Information
  - Bearbeitung ist gesetzlich vorgesehen
  - Gesetzliche Geheimhaltungsverpflichtung
  - Sofern die Personendaten nicht bei der betroffenen Person beschafft werden, so entfällt Informationspflicht, wenn die Information nicht möglich ist

Was bedeutet dies in der Praxis?

-> Nichteinhaltung kann strafrechtliche Sanktionen nach sich ziehen

-> Wenn Sie auf die Information verzichten, klären Sie ab, ob dies keine Verletzung der Informationspflicht ist und dokumentieren Sie diesen Entscheid

-> Erarbeiten Sie Datenschutzerklärungen oder integrieren Sie die Informationen in Ihre Verträge (z.B. Arbeitsverträge, AGB), um der Pflicht nachzukommen

Automatisierte Einzelentscheidungen

Was sagt das Recht?

- Erweiterte Informationspflicht betreffend automatisierte Einzelentscheidungen
- Betroffene Personen müssen ihren Standpunkt darlegen können

Was bedeutet dies in der Praxis?

-> Die Einführung von Automatisierungsprozessen sind immer mit Blick auf den Datenschutz umzusetzen

Datenschutz-Folgeabschätzungen

Was sagt das Recht?

- Der Verantwortliche hat eine Datenschutz-Folgeabschätzung zu erstellen, wenn ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen besteht
  - Umfangreiche Bearbeitung von besonders schützenswerten Personendaten
  - Systematische umfangreiche öffentliche Bereich überwacht werden
- Gegebenenfalls ist der EDÖB zu konsultieren

Was bedeutet dies in der Praxis?

-> Bei der Einführung neuer Bearbeitungsprozesse sollte sich ein Unternehmen die Frage stellen, ob eine Datenschutz-Folgeabschätzung erstellt werden muss

-> Der Prozess kann auch die notwendigen technischen und organisatorischen Massnahmen identifizieren helfen

Meldung von Datenschutzverletzungen

Was sagt das Recht?

- Eine Datensicherheitsverletzung muss dem EDÖB so rasch wie möglich gemeldet werden, wenn
  - Hohes Risiko für die Persönlichkeit der betroffenen Personen
  - Hohes Risiko für die Grundrechte der betroffenen Personen
- Mindestumfang der Meldung vom Gesetz vorgegeben
- Meldungspflicht des Auftragsbearbeiters an den Verantwortlichen
- Gegebenenfalls darüber hinausgehende vertragliche Meldepflichten
- Gegebenenfalls Information an die betroffenen Personen

Was bedeutet dies in der Praxis?

-> Es ist sinnvoll, den Ernstfall in unternehmensinternen Prozessen zu dokumentieren, um eine rasche Meldung trotz Schwierigkeiten (z.B. fehlender Zugriff auf das System) sicherzustellen

-> Eine klare Hierarchie und Zuständigkeitsmatrix hilft bei der raschen Behandlung des Datensicherheitsvorfalls

-> Mitarbeiter sind für den Fall einer Datensicherheitsverletzung zu Schulen

-> Bei der Meldung an den EDÖB sind allfällige haftungsrechtliche Problematiken zu berücksichtigen

-> Ein schlechtes Management des Datensicherheitsvorfalls kann auch einen Reputationsschaden nach sich ziehen

BETROFFENENRECHTE

Was sagt das Recht?

- Recht auf Auskunft
- Recht auf Datenherausgabe und -übertragung
- Recht auf Berichtigung unrichtiger Personendaten
- Recht auf einen Bestreitungsvermerk
- Recht auf Löschung
- Recht auf Sperrung

Was bedeutet dies in der Praxis?

-> Es ist sinnvoll klare Prozesse zu definieren

-> Eine Übersicht der Datenbearbeitungsaktivitäten hilft Anfragen zu beantworten

-> Anfragen sind in der Regel unentgeltlich zu erbringen, daher ist eine gute Planung unabdingbar zur Schonung von Kosten und Ressourcen (ausnahmsweise kann eine Entschädigung bis CHF 300 verlangt werden)

-> Anfragen sind in der Regel innerhalb von 30 Tagen zu beantworten

KOMPETENZEN DES EDÖB

Was sagt das Recht?

- Kompetenzen des EDÖB wurden stark erweitert
  - Untersuchungen einleiten
  - Zugang zu allen erforderlichen Auskünften, Unterlagen, Verzeichnissen der Bearbeitungstätigkeiten und Personendaten verlangen
  - Zugang zu Räumlichkeiten und Anlagen verlangen
  - Zeugeneinvernahmen durchführen
  - Begutachtungen durch Sachverständige veranlassen
  - Verwaltungsmassnahmen (Anpassung, Unterbrechung oder Unterlassung von Bearbeitungstätigkeiten, Löschung oder Vernichtung von Personendaten anordnen) erlassen
  - Verwarnungen aussprechen

Was bedeutet dies in der Praxis?

-> Es gibt noch keine Behördenpraxis

-> EDÖB wird wohl eine grössere Rolle spielen wollen

-> EDÖB baut personelle Ressourcen zur Zeit aus

-> Nichtbefolgung einer Anordnung des EDÖB ist strafbewehrt

Sanktionen

Was sagt das Recht?

Strafbar sind…

- … Verletzung von Information-, Auskunfts- und Mitwirkungspflichten
- … Verletzung von Sorgfaltspflichten
- … Verletzung der beruflichen Schweigepflicht
- … Missachten von Verfügungen
- … Widerhandlungen in Geschäftsbetrieben

Was bedeutet dies in der Praxis?

-> Das Datenschutzrecht bekommt bissige Sanktionen

-> Strafbar sind in erster Linie Privatpersonen und nicht das Unternehmen

-> Umsetzung wird zur Sache der Entscheidungsträger

DOKUMENTATIONSPFLICHTEN

Was sagt das Recht?

- Das Gesetz sieht keine generelle Dokumentationspflicht vor, allerdings sind bestimmte Pflichten notwendigerweise festzuhalten

Was bedeutet dies in der Praxis?

-> Vorgeschriebene Dokumente sind aktuell zu halten

-> Im Rahmen von Datenbearbeitungen sind klare Dokumentationsprozesse zu definieren

-> Die Dokumentation bestimmter Entscheidungen kann haftungsmindernd sein

-> Dokumentation hilft im Ernstfall, zum Beispiel kann ein gutes IKS die Umsetzung der Datensicherheit gemäss dem «State of the Art» dokumentieren

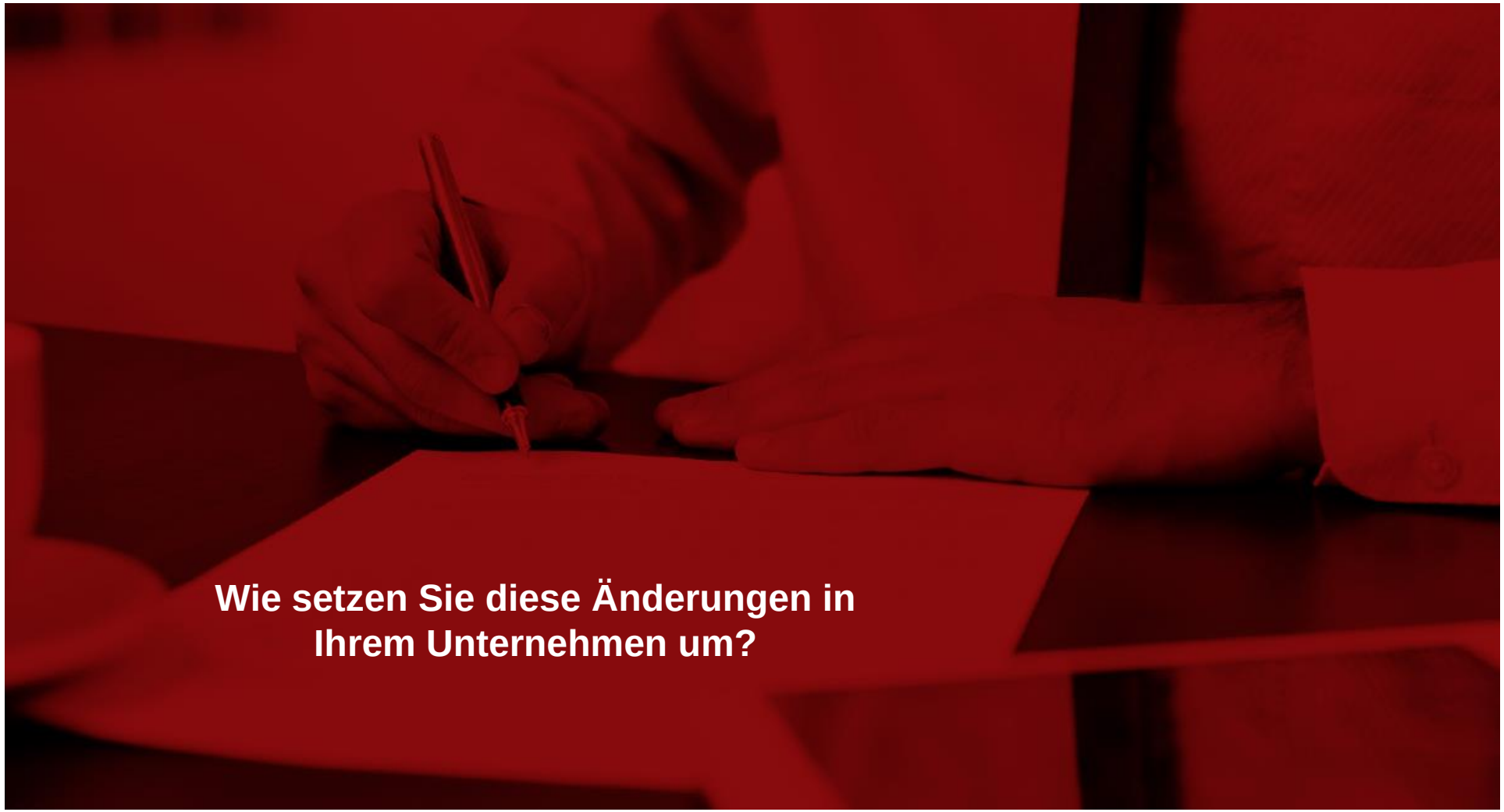
Datenschutz ist Sache der Entscheidungsträger

Verletzungen des DSG ziehen strafrechtliche Sanktionen nach sich

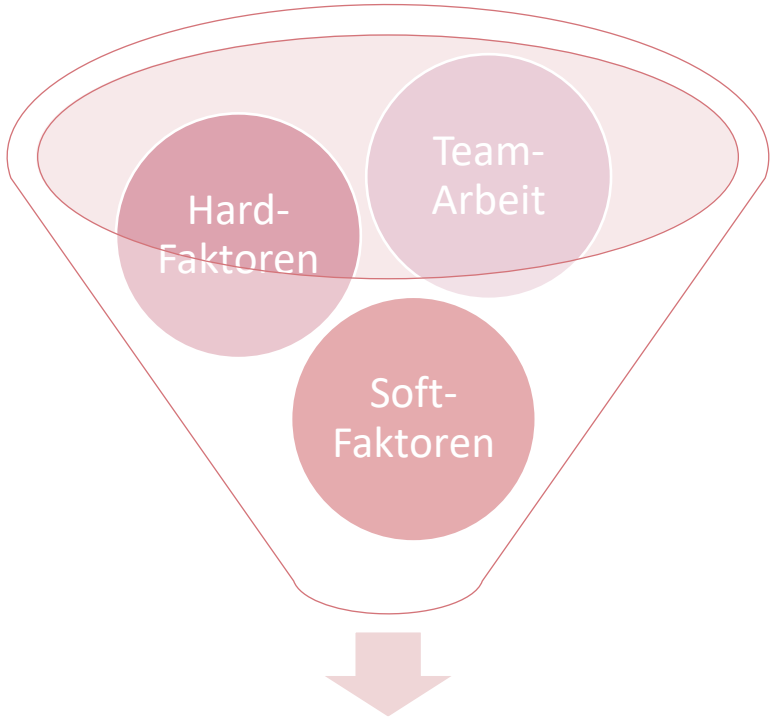
- Bei einer Verletzung von Informations-, Auskunfts- und Mitwirkungspflichten werden **private Personen** auf Antrag mit Busse bis zu CHF 250'000.00 bestraft
- Bei einer Verletzung von Sorgfaltspflichten werden **private Personen** auf Antrag mit Busse bis zu CHF 250'000.00 bestraft
- Bei einer Verletzung der beruflichen Schweigepflicht werden private Personen auf Antrag mit Busse bis zu CHF 250'000.00 bestraft
- Beim Missachten von Verfügungen werden **private Personen** auf Antrag mit Busse bis zu CHF 250'000.00 bestraft
- In Ausnahmefällen Strafbarkeit des Geschäftsbetriebs anstelle der privaten Person

DSG-Compliance schafft auch Mehrwert

- Erkenntnisgewinn (Übersicht über Prozesse und Datenbanken und Kenntnis über allfällige Doppelspurigkeit bei Systemen)
- Effizienzgewinn (Vereinfachung von Prozessen, klare Definition der verantwortlichen Personen und dadurch Einsparung von Kosten)
- Risikomanagement (Identifizierung von Risiken und Möglichkeit der Implementierung von risikominimierenden Massnahmen)
- Enabler-Funktion (weniger Einschränkungen im Tagesgeschäft)
- Wettbewerbsvorteil (sowohl gegenüber Kunden wie auch bei der Rekrutierung neuer Mitarbeiter)
- Klare Prozesse im Ernstfall (z.B. bei einer Cyberattacke oder im Rahmen einer Streitigkeit mit einem gekündigten Mitarbeiter)


Wie setzen Sie diese Änderungen in
Ihrem Unternehmen um?

Zutaten für eine erfolgreiche DSG-Umsetzung



- Team-Arbeit
  - Wissen von verschiedener Abteilungen (insbesondere Fachverantwortliche IT, Konzerngesellschaften und Vertragspartner) notwendig
  - Rechtliche Unterstützung (Ausarbeitung bzw. Aktualisierung Verträge oder Ausarbeitung von Prozessen, Richtlinien und Weisungen)
  - Knowhow DSG, Betrieb, Marktumfeld und Behördenpraxis
  - Management für die Implementierung des Projekts
- Hard-Faktoren
  - Zeit
  - Ressourcen
  - Organisation
  - Knowhow
  - Implementierung
  - Dokumentation
- Soft-Faktoren
  - Motivation
  - Nutzen
  - Bekenntnis Unternehmensleitung zur Umsetzung
  - Unternehmenskultur und Risikobewusstsein

Planung des Umsetzungsprojekts

Haben Sie die Zeit bis zum Inkrafttreten im Blick

Prüfen Sie welche Ressourcen Sie intern sowie extern zur Verfügung haben

- Ziehen Sie einen Sparring-Partner zur Unterstützung bei
- Sichern Sie sich die Unterstützung der IT
- Komplette Auslagerung allerdings nicht sinnvoll, da das DSG im Unternehmen umgesetzt werden muss

Machen Sie eine Bestandesaufnahme (Knowhow, bestehende Dokumentation, Datenverarbeitungen)

- Ggf. Erstellen einer Gap-Analyse

Erarbeiten Sie ein Plan für die etappenweise Umsetzung

- Priorisieren Sie bestimmte Arbeiten
- 100% Compliance ist nicht möglich, handeln Sie daher gemäss einem risikobasierten Ansatz

Schulen Sie Ihre Mitarbeiter

Vorschlag für eine Priorisierung bei der Umsetzung

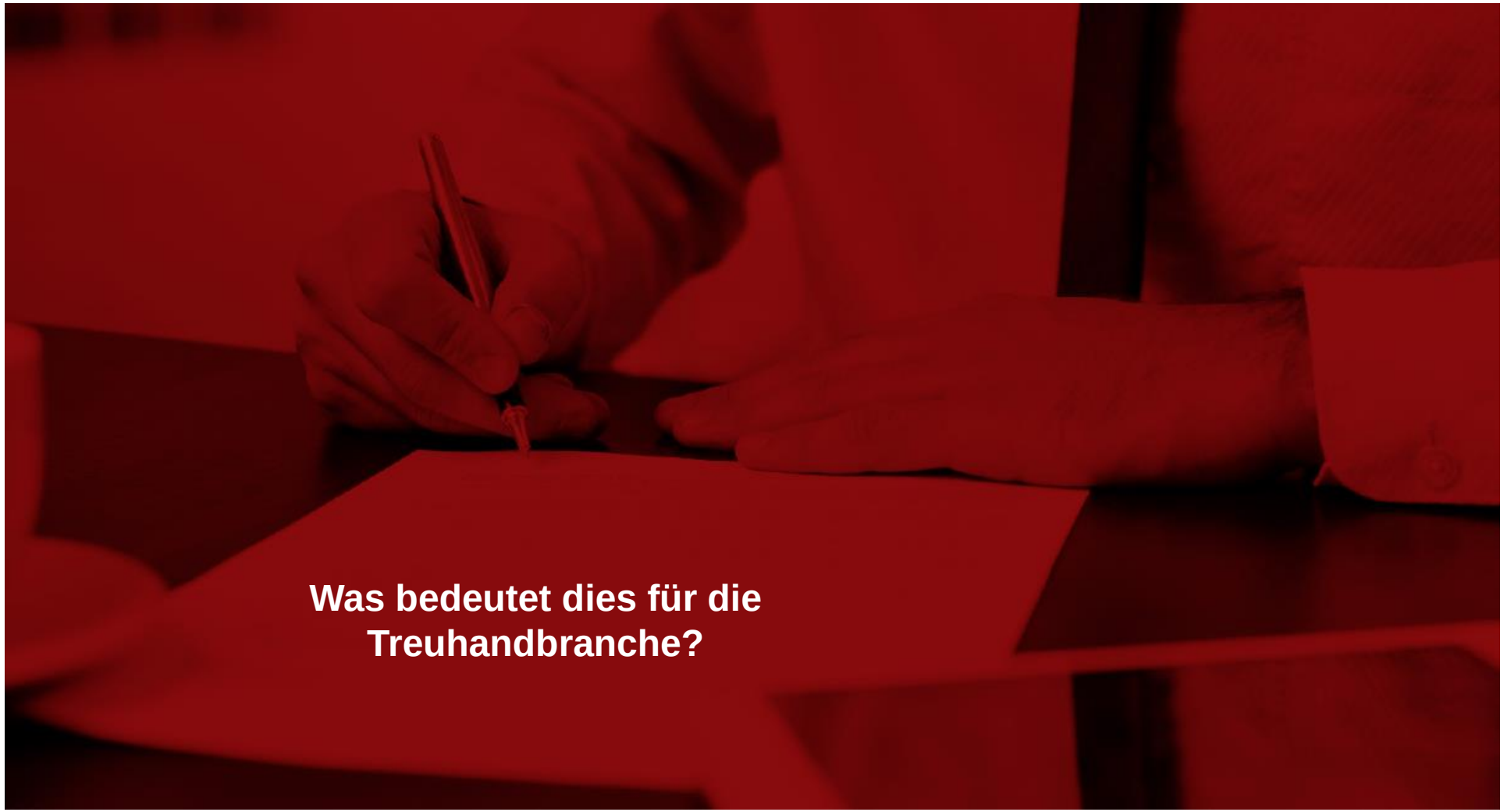
- Verletzung von Information-, Auskunfts- und Mitwirkungspflichten
- Verletzung von Sorgfaltspflichten (insbesondere betr. Auftragsbearbeitung)
- Verletzung der beruflichen Schweigepflicht
- Missachten von Verfügungen
- Widerhandlungen in Geschäftsbetrieben

Welche Fragen müssen Sie sich konkret stellen?

- Welche Gesellschaften werden bei der Umsetzung berücksichtigt?
- Welche Bearbeitungstätigkeiten erbringt das Unternehmen?
- Wurde die DSGVO bereits umgesetzt?
- Soll ein Datenschutzberater bestimmt werden?
- Braucht es einen Schweizer Vertreter?
- Ist ein Bearbeitungsverzeichnis zu erstellen?
- Besteht eine Übersicht der Datenbearbeitungen?
- Wurden alle notwendigen Datenschutzerklärungen ausgearbeitet?
- Bestehen Auftragsbearbeitungsverträge? Wenn ja, müssen diese überarbeitet werden?
- Wurden die AGB bereits aufgrund des revDSG aktualisiert?
- Besteht eine konzerninternen Datentransfervereinbarung? Ist diese aktuell?
- Muss eine Datenschutzfolgeabschätzung erstellt werden?
- Gibt es Datenbekanntgaben ins Ausland?
- Sind die Anforderungen an Datenbekanntgaben erfüllt? Muss zum Beispiel noch ein Transfer Impact Assessment erstellt werden?
- Wurden angemessene technischen und organisatorischen Massnahmen implementiert?
- Wurden alle notwendigen internen Weisungen und Reglemente erlassen und implementiert?
- Gibt es eine Datenaufbewahrungsrichtlinie? Muss diese noch aktualisiert werden?
- Besteht ein Prozess zur Meldung von Datenschutzverletzungen?
- Besteht ein Prozess zur Beantwortung von Betroffenenrechten?
- Werden die Mitarbeiter regelmässig geschult?
- Wurde eine regelmässige Überprüfung und Aktualisierung der Compliance-Dokumente im Unternehmen implementiert?

Sinnvolle Dokumente bzw. Nachweise zur Beantwortung der vorstehenden Fragen

- Datenschutzweisung inkl. Governance
- IT-Weisung inkl. Überwachung
- Aufbewahrungsrichtlinie
- Vertraulichkeitserklärung Mitarbeitende
- Spezialweisung zum Umgang mit Verletzung der Datensicherheit
- Spezialweisung für Begehren von betroffenen Personen
- Spezialweisung für Fachbereiche (HR, Marketing)
- Weisung betreffend Informationssicherheit
- Schulungsdokumente für Mitarbeitende
- Awareness-Trainings
- Merkblatt Do's and Don'ts für Mitarbeitende
- Merkblätter für bestimmte Fachbereiche (z.B. HR und Marketing)
- Bearbeitungsverzeichnis (ROPA)
- Bearbeitungsreglement
- Verzeichnis von Datensicherheitsvorfällen
- Dokumentation Betroffenenbegehren
- Standardantworten für Anfragen
- Datenschutzerklärungen (z.B. Webseite, Mitarbeiter, Rekrutierungsplattformen)
- Cookie & Consent Management
- Nachweis von Compliance-Prüfung
- Datenschutz-Folgenabschätzung
- Transfer Impact Assessments (TIA) bei heiklen Datentransfers
- Auftragsbearbeitungsvertrag (ADV)
- Übersicht technische und organisatorische Massnahmen (TOMs)
- Inter-Company Vertrag bei Gruppengesellschaften
- Standardvertragsklauseln für Verträge mit Kunden und/ oder Lieferanten
- Datenschutz-Reporting (z.B. als Teil des IKS)


Was bedeutet dies für die
Treuhandbranche?

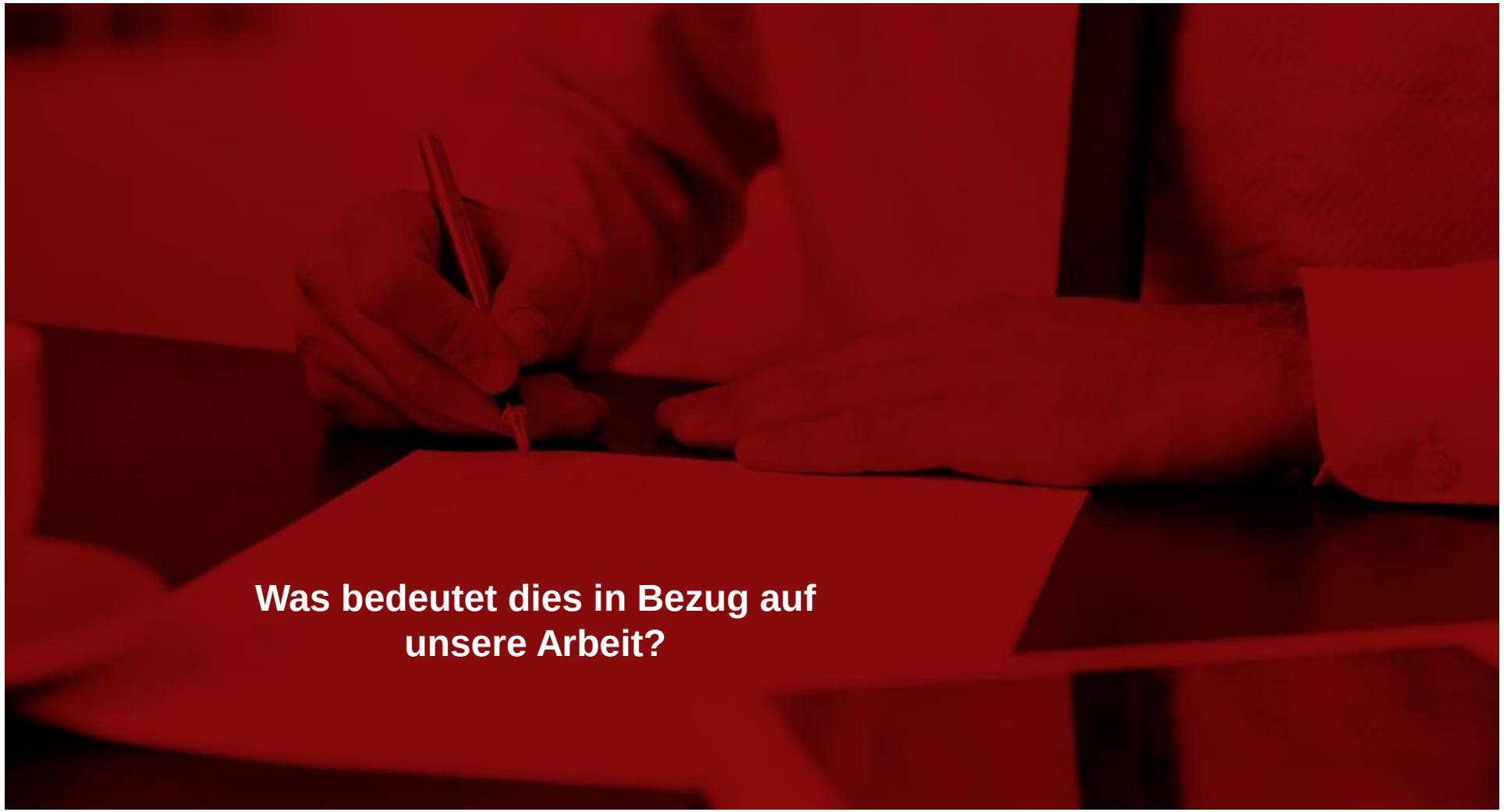
Was bedeutet dies für mein Unternehmen?

Im Innenverhältnis

- Das DSG findet auf die Treuhandbranche Anwendung
- Die Zeit läuft und das Gesetz entfaltet ab dem 1. September 2023 Wirkung
- Sofern mit der Umsetzung noch nicht begonnen wurde, ist eine Priorisierung der Massnahmen vorzunehmen
- Vorbereitung hilft und schont Kosten
- Datenschutz kann Mehrwert bringen, wenn eine Unternehmen diesen sinnvoll implementiert

Nach Aussen

- Machen Sie Ihre Kunden auf das angepasste Recht aufmerksam
- Agieren Sie proaktiv, um sich einen Wettbewerbsvorteil zu verschaffen
- Unterstützen Sie Ihre Kunden bei der Umsetzung (z.B. im Rahmen der internen Revision)
- Aktualisieren Sie Ihre Verträge mit Ihren Kunden


Was bedeutet dies in Bezug auf
unsere Arbeit?

Key Take-Aways für den Alltag

Für das eigene Unternehmen

- Die Arbeit bleibt dieselbe
- Gestärktes Bewusstsein für den Wert von Daten
- Erhöhte Dokumentationspflichten
- Erhöhte Transparenz und Bewusstsein über die Arbeitsprozesse
- Möglichkeit der Effizienzgewinne
- Hohes Level an Datenschutz als «selling» Kriterium

Für die Kunden

- Schafft Vertrauen gegenüber dem Treuhänder
- Schafft Transparenz
- Zeigt Kompetenz des Treuhänders
- Ermöglicht dem Unternehmen das Gespräch mit dem Kunden zu suchen

Haben Sie Fragen oder Anmerkungen?

Ihr Kontakt

Cornelia Mattig, LL.M.

Roesle Frick & Partners
Bleicherweg 18
8002 Zürich
Schweiz

cornelia.mattig@rfplegal.ch

ROESLE FRICK & PARTNER

ZÜRICH

Bleicherweg 18
Postfach
8027 Zürich
Tel +41 43 344 22 22
Fax +41 43 344 22 11
rfpzh@rfplegal.ch

PFÄFFIKON/SZ

Churerstrasse 135
Postfach 228
8808 Pfäffikon SZ
Tel +41 55 416 26 36
Fax +41 55 416 26 37
rfpsz@rfplegal.ch