VISCHER

EU-DSGVO ante Portas
Was gilt und was zu tun ist

Workshop und Guidelines für IAB Switzerland

VISCHER AG, Zürich, 7. Dezember 2017

Dr. Rolf Auf der Maur
Dr. Thomas Steiner, LL.M.

Überblick

- Regelungszweck und Treiber des Datenschutzes
- DSGVO auf einen Blick
- DSGVO-Compliance: Umsetzung im Unternehmen
- Ausblick: Gesetzesrevision in der Schweiz und EU e-Privacy Verordnung

Regelungszweck und Treiber des Datenschutzes

Regelungsinteresse beim DSG 1992: Schutz vor dem Überwachungsstaat

Regelungsinteresse beim DSG 1992: Schutz vor dem Überwachungsstaat

- Schutz der Persönlichkeit (Private und Unternehmen)
- Schutz vor dem Staat ("Fichenaffäre" 1989)
- Föderalismus (DSG für Private und Bund, kantonale Gesetze für kantonale Behörden)
- Technologischer Stand: Nachkriegszeit
- Schweiz 1992 als "Nachzügler" in Europa

Treiber der DSG Revision 2017: Angst vor Kontrollverlust bei Big Data Analytics

Treiber der DSG Revision 2017: Angst vor Kontrollverlust bei Big Data Analytics

- Daten als Rohstoff für digitale Geschäftsmodelle
- Big Data und Data Analytics auf dem Vormarsch
- Migration von Daten in die "Cloud"
- Wachsende Risiken für die Datensicherheit
- Algorithmen übernehmen Selektionen und führen automatisierte Entscheide aus

Unterschied Daten/Personendaten

Informationen	Ohne jeglichen Personenbezug
Anonyme Daten	Betroffene Person kann nicht mehr identifiziert werden
Pseudonyme Daten	Ohne zusätzliche Informationen keine Zuordnung der Daten möglich
Personendaten	Beziehen sich auf identifizierte oder identifizierbare natürliche Person

Datenschutz: Was ist neu in der EU?

- EU-DSGVO ab 25. Mai 2018 mit hoher Bussendrohung (bis 4% des Jahresumsatzes weltweit oder EUR 20 Mio.)
- Höhere Anforderungen an Transparenz (Informationspflichten) und Kontrollmöglichkeiten (Einwilligung und Widerruf der Einwilligung)
- Datenschutz beinhaltet neu auch konkrete Anforderungen an Datensicherheit und Transparenz bei Data Breaches (Notifikation gegenüber Behörden und Betroffenen)
- e-Privacy Verordnung in Vorbereitung und heftig umstritten

Was gilt in der Schweiz?

- EU-DSGVO ist ab 25. Mai 2018 auch für die meisten Schweizer Unternehmen anwendbar, sofern sie
  - natürlichen Personen in der EU Produkte oder Dienstleistungen anbieten (entgeltlich oder unentgeltlich)
  - das Verhalten von Nutzern ihrer Website/App aus der EU analysieren
  - an der Datenverarbeitung von EU-Unternehmen teilnehmen (z.B. als Auftragsverarbeiter oder als Schweizer Konzerngesellschaft)
- Entwurf zur Teilrevision des DSG vom 15. September 2017 zur Zeit in der parlamentarischen Beratung (Ziel: Erhalt der Gleichwertigkeit gegenüber EU, aber teilweise überschiessend, besonders bezüglich «Profiling»)

DSGVO auf einen Blick

DSGVO Regelungsthemen auf einen Blick

Anwendbarkeit EU-DSGVO

Rechtmässige Verarbeitung (insb. Einwilligung)

Transparenz (Informations-pflichten)

Rechte der Betroffenen

Dokumenta-tionspflichten

Auftragsdaten-verarbeitung

Auslands-datentransfer

Profiling / automat. Einzel-entscheide

Datenschutz-Folgen-abschätzung

«Data Breach» Meldepflicht

Datensicherheit und Privacy by Design & Default

«Governance»

Checkliste - Zusammenfassung

Thema	Massnahmen (bis 25. Mai 2018)
	Prüfen, ob ihr Unternehmen Personendaten verarbeitet; prüfen, ob Ihr Unternehmen Dienstleistungen an Personen (Individuen) in der EU anbietet oder das Verhalten von Nutzern analysiert, die sich in der EU befinden (Art. 2(1), 3(2) und 4(1))
	Prüfen, auf welcher Grundlage (insb. Erfüllung eines Vertrags, legitime und überwiegende Interessen, Einwilligung) Ihr Unternehmen Personendaten verarbeitet; Prozesse zur Einholung, Dokumentation und Verwaltung (inkl. Widerrufs-möglichkeit) von Einwilligungen anpassen bzw. einführen (Art. 6–8)
	Bestehende Datenschutzerklärungen prüfen und anpassen (Mindestinhalt gemäss 13–14)
	Prozesse zur Gewährung der Rechte auf Auskunft, Berichtigung, Einschränkung, Löschung, Datenportabilität und Widerspruch überprüfen/anpassen/einführen (Art. 15–23)
	Zentrales Verzeichnis zur Dokumentation aller Datenverarbeitungsprozesse einführen; inkl. Kategorien, Herkunft und Übermittlung der Personendaten (Art. 30); prüfen ob Ausnahme für «KMU» greift
	Datenverarbeitungs-/Datentransferverträge überprüfen und anpassen; Verantwortlichkeiten und Risiken von Verantwortlichen und Auftragsverarbeiter definieren (Mindestgemäss Art. 28(3))
	Identifizierung von Auslandsdatentransfers; Übermittlungsprozesse und -grundlagen prüfen und anpassen; Datentransfer-verträge prüfen und anpassen (Art. 44–50)
	Automatisierte Einzelfallentscheide basierend auf Profiling: Recht auf Intervention gewähren (Art. 22); Profiling als Grundlage für Entscheidungen mit Rechtswirkung oder erheblicher Beeinträchtigung: Datenschutzfolgenabschätzung (Art. 35(3)(a))
	Prozesse zur Durchführung und Dokumentation von Datenschutz-Folgenabschätzungen (Art. 35) bzw. der vorherigen Konsultation der Aufsichtsbehörde (Art. 36) prüfen/anpassen/einführen
	Prozesse zur Identifizierung/Untersuchung/Meldung von «Data Breaches» prüfen/anpassen/einführen (Art. 33–34)
	Bestehende technische und organisatorische Sicherheitsmassnahmen überprüfen / anpassen; interne Richtlinien / Schulungen überprüfen / anpassen (Art. 32); Privacy by Design & Default risikobasiert umsetzen (Art. 25)
	Datenschutzbeauftragte und Vertreter in der EU ernennen, Kompetenzen festlegen, Kontaktdaten veröffentlichen und der Aufsichtsbehörde melden (Art. 37–39); Dokumentationspflichten einhalten, insb. Verzeichnis der Verarbeitungstätigkeit führen (Art. 30)

DSGVO-Compliance: Umsetzung im Unternehmen

Anwendbarkeit EU-DSGVO

Fragen	Massnahmen	Erläuterung
Verarbeiten wir Personendaten?	✓ Datenverarbeitungsprozesse inhaltlich prüfen (Datenkategorien analysieren) ✓ Personendaten, wo immer möglich, anonymisiert/pseudo-nymisiert verarbeiten ✓ Bewusstsein schaffen ✓ Auswirkungen von Verletzungen verstehen ✓ Risikobeurteilung durchführen	Betroffene Daten: EU-DSGVO nur anwendbar, wenn Personendaten verarbeitet werden
• Bieten wir unsere Dienst-leistungen Personen (Individuen) in der EU an? • Beobachten wir das Verhalten von Nutzern unserer Website/App, die die sich in der EU befinden? • Nehmen wir an der Datenverar-beitung von EU-Unternehmen teil		Unternehmen in der Schweiz betroffen

Rechtmässige Verarbeitung (insb. Einwilligung)

Fragen	Massnahmen	Erläuterung
• Verarbeiten wir Personendaten basierend auf Einwilligungen? • Holen wir Einwilligungen separat oder zusammen mit dem Akzept des Angebots/der AGB ein?	✓ Prozesse zur Einholung, Dokumentation und Verwaltung von Einwilligungen prüfen/anpassen/einführen ✓ Bestehende Einwilligungen und Datenschutzerklärungen prüfen/ anpassen ✓ Prüfen, ob Voraussetzungen zur Verarbeitung besonders schützenswerter Personendaten erfüllt sind ✓ Prüfen, ob insb. die Notwendigkeit zur Vertragserfüllung oder überwiegende legitime Interessen als Alternative Grundlage für die Rechtmässigkeit der getätigten/ geplanten Datenverarbeitung dienen kann	Gültige Einwilligung: freiwillig und eindeutig, auf informierter Basis, nicht an andere Zustimmungen gekoppelt
Haben wir einen standardisierten Prozess zur Einholung, Dokumentation und Verwaltung (inkl. Widerrufsmöglichkeit und Meldung von Widerrufen an Dritte)?		• Unternehmen muss nachweisen können, dass die betroffene Person die Einwilligung erteilt hat • Einwilligung muss jederzeit leicht widerrufbar sein • Unternehmen muss Betroffene auf Widerrufsrecht aufmerksam machen und Widerruf auch umsetzen können, wenn Daten an Dritte bekannt gegeben worden sind
Verarbeiten wir Personendaten basierend auf anderen Erlaubnistatbeständen / Grundlagen?		Andere Grundlagen: insb. Vertragserfüllung und überwiegende legitime Interessen

Transparenz (Informationspflichten)

Fragen	Massnahmen	Erläuterung
Wie informieren wir über die Erhebung und Verarbeitung von Personendaten und wann?	✓ AGB prüfen/anpassen ✓ Datenschutzerklärung prüfen/anpassen, sodass sie den Mindestinhalt gemäss DSGVO enthält ✓ Verwendung von Piktogrammen/Bildern prüfen ✓ Datenschutzerklärungen übersichtlich mit sog. «Layered Notices» und Kontrollmöglichkeiten (im Online Kundencenter) gestalten	EU-DSGVO verlangt weitgehende Information der Betroffenen im Zeitpunkt der Erhebung bzw. innert einem Monat nach Erhalt (wenn bei Dritten erhoben)
Informieren wir über die Aufbewahrungs-dauer von Personendaten («Datenmini-mierungsprinzip»)?		
Beantworten wir folgende Fragen mit unserer Datenschutzerklärung: «Wer verarbeitet was zu welchem Zweck für wie lange und welche Rechte ergeben sich daraus für den Betroffenen»?		Die EU-DSGVO (Art. 13 und 14) enthält eine lange Liste mit Mindestanforderungen an die Information
Ist unsere Datenschutzerklärung verständlich, leicht zugänglich, klar und einfach?		
Verwenden wir Bildsymbole / gestaffelte Datenschutzerklärungen?		

Rechte der Betroffenen

Fragen	Massnahmen	Erläuterung
Haben wir standardisierte Prozesse für: • die Gewährung des Auskunftsrechts? • die Sicherstellung der Richtigkeit der Personendaten? • die Gewährleistung der Datenportabilität? • die Einschränkung der Verarbeitungsprozesse? • die Überprüfung der Notwendigkeit von Personendaten? • die Löschung von Personendaten, die nicht mehr benötigt werden? • den Widerspruch gegen eine Datenverarbeitung?	✓ Simple/standardisierte Prozesse zur Gewährung der Rechte überprüfen/ anpassen/einführen ✓ Prozesse zur raschen Auskunftserteilung sicherstellen ✓ Templates für Gesuche überprüfen/anpassen/ einführen	• Betroffene haben Auskunfts-, Berichtigungs-, Einschränkungs-, Löschungs- und Widerspruchsrecht • Betroffene haben Recht auf Datenportabilität
Informieren wir über diese Rechte? Wie?		Betroffene müssen über diese Rechte informiert werden
Haben wir einen internen Datenschutzbeauftragten / eine interne Anlaufstelle für solche Anfragen?		Betroffene müssen ihre Rechte leicht geltend machen können

Dokumentationspflichten

Fragen	Massnahmen	Erläuterung
• Dokumentieren wir unsere Datenverarbeitungsprozesse? • Was deckt unsere bestehende Dokumentation ab?	✓ Einführung zentrales Verzeichnis zur Dokumentation aller Datenverarbeitungsprozesse (Verzeichnis gemäss Art. 30 führen) ✓ Einführung/Anpassung der internen Datenschutzrichtlinie ✓ Dokumentation bereit halten, die zeigt, wie Datenschutz gelebt wird (Richtlinien, Weisungen, Schulungen, Merkblätter, Webinars, Fragebogen etc.) ✓ Periodische Überprüfung der Datenschutz-Compliance	Umfassende Rechenschaftspflicht (insbesondere bzgl. Datensicherheit) • Datenverarbeitungen sind von A-Z schriftlich zu dokumentieren (z.B. Information der Betroffenen, Verarbeitungsschritte, Datenübermittlungen, Sicherheitsmassnahmen, Einwilligungen, Data Breaches, DSFAs etc.) • Ausnahme von der Verzeichnispflicht für KMU (unter 250 Mitarbeiter), es sei denn, die Verarbeitungen sind risikobehaftet

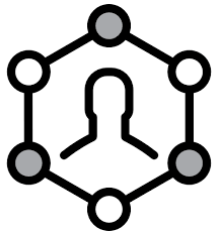
Auftragsverarbeitung

Fragen	Massnahmen	Erläuterung
• Nehmen wir Auftragsverarbeiter in Anspruch? • Sind wir als Auftragsverarbeiter tätig?	✓ Vertragsmuster / Muster-klauseln für Verträge mit Auftragsverarbeitern definieren ✓ Identifizierung relevanter Verträge / Vertragspartner ✓ Datenverarbeitungs- / Datentransferverträge risikobasiert prüfen / anpassen ✓ Verantwortlichkeiten und Risiken von Verantwortlichen und Auftragsverarbeitern definieren	
Bestehen zwischen dem jeweiligen Verantwortlichen und dem jeweiligen Auftragsverarbeiter schriftliche Verträge mit dem Mindestinhalt gemäss Art. 28(3)?		EU-DSGVO definiert den Mindestinhalt von Datenverarbeitungsverträgen
Welchen Sicherheitsstandard garantieren Auftragsnehmer / garantieren wir Auftragsgebern?		Anforderungen an die Datensicherheit sind eines der wichtigsten Regelungsthemen im Vertrag betreffend Auftrags-verarbeitung
Dokumentieren wir die sorgfältige Auswahl und Überwachung von Auftragsverarbeitern?		EU-DSGVO legt gemeinsame Verantwortlichkeiten für Verantwortliche und Auftragsverarbeiter fest

Auslandsdatentransfer

Fragen	Massnahmen	Erläuterung
• Verarbeiten wir Personendaten im Ausland? • Wo liegen unsere Server?	✓ Identifizierung von Auslandsdatentransfers ✓ Übermittlungsprozesse / -grundlagen prüfen/an-passen ✓ Datentransferverträge prüfen / anpassen	Auslandsdatentransfers grundsätzlich zulässig, wenn Drittland angemessenes Datenschutzniveau bietet (Angemessenheitsbeschlüsse EU Kommission)
Auf welcher Grundlage transferieren wir Personendaten ins Ausland?		Wenn kein Angemessenheits-beschluss, andere Garantien notwendig (insb. Model Clauses, Binding Corporate Rules)
• Transferieren wir Personendaten in die USA? • Sind die Verarbeiter in der USA gemäss Privacy Shield-zertifiziert?		An Privacy Shield-zertifizierte Unternehmen müssen Anforderungen an den Datenschutz einhalten, die als gleichwertig bzw. angemessen gelten

Profiling / automat. Einzelentscheide



Fragen	Massnahmen	Erläuterung
• Verarbeiten wir Personendaten vollständig automatisiert? • Betreiben wir Profiling?	✓ Automatisierte Prozesse prüfen/anpassen ✓ Überprüfen, welche Wirkungen diese Prozesse entfalten ✓ Prozess zur Information und Intervention einführen, wo auf der Grundlage von Profiling automatisiert Einzelfallentscheide mit Rechtswirkung oder ähnlicher Wirkung getroffen werden ✓ Datenschutzfolgenab-schätzung durchführen, wenn mit der geplanten Verarbeitung auf der Grundlage von Profiling Entscheide mit Rechtswirkung oder Wirkung getroffen werden sollen	Profiling ist zulässig, sofern nicht mit automatisiertem Einzelfallentscheid mit rechtlicher/tatsächlicher Wirkung für den Betroffenen verbunden
• Fällen wir Einzelentscheide basierend auf Profiling? • Fällen wir basierend auf Profiling automatisierte Einzelfallentscheide mit Rechtswirkungen oder ähnlicher Wirkung? • Haben wir standardisierte Prozesse zur Information der Betroffenen und um die Wahrnehmung von Eingriffs- und Anfechtungsrechten zu ermöglichen? • Führen wir vor risikobehafteten Verarbeitungen basierend auf Profiling eine Datenschutzfolgenabschätzung durch?		• Datenschutzfolgenabschätzung bei Entscheiden basierend auf Profiling mit rechtlichen/tatsächlichen Wirkungen • Informations- und Anhörungspflicht bei automatisierten Einzelfallentscheiden mit rechtlichen/tatsächlichen Wirkungen

Datenschutz-Folgenabschätzung (DSFA)

Fragen	Massnahmen	Erläuterung
• Setzen wir neue Technologien/Apps/ Software/neue Datenverarbeitungs-methoden ein? • Wer entscheidet, darüber ob eine geplante Verarbeitung durchgeführt werden kann?	✓ Bestehende DSFA prüfen/ anpassen ✓ DSFA einführen, falls noch nicht besteht ✓ Dokumentation der DSFA sicherstellen ✓ Periodische Überprüfung	Zeitpunkt: vor Beginn einer geplanten/neuen Verarbeitung
Birgt die Datenverarbeitung ein Risiko/hohes Risiko?		Durchführen, wenn hohes Risiko für Rechte/Freiheiten des Betroffenen besteht
• Welche Prozesse bestehen schon? • Wie werden die Ergebnisse ausgewertet (systematisch, automatisch etc.)?		DSFA müssen dokumentiert werden
		Konsultationspflicht bei Aufsichtsbehörde, wenn Risiko nicht eindämmbar

«Data Breach» Meldepflichten

Fragen	Massnahmen	Erläuterung
• Wie/an wen melden wir Data Breaches? • Gibt es Prozesse, um Schutzverletzungen zu entdecken (auch beim Auftragsverarbeiter)? • Ermöglichen diese Prozesse, Data Breaches innert 72h zu melden?	✓ Meldeprozesse prüfen/ anpassen ✓ Prozesse zur Identifizierung und Untersuchung von Ereignissen prüfen/ anpassen ✓ Richtlinie zur Behandlung von Data Breaches einführen	Meldepflicht an Aufsichtsbehörde Frist: 72h (bei hohem Risiko Meldung auch umgehend an Betroffene)
Gibt es Prozesse, um zu entscheiden ob ein Risiko/ein hohes Risiko für die Rechte und Freiheiten des Betroffenen bestehen?		Risiko prüfen weil: Meldepflicht an Behörde bei risikobehaftetem Data Breach / Meldung an Betroffene nur bei hohem Risiko
• Haben wir Prozesse, um die Folgen von Data Breaches nachzuvollziehen? • Können wir die Auswirkungen messen? • Führen wir eine Liste der Schutz-verletzungen?		Inhalt der Meldung: Art der Verletzung, Kategorien/Zahl der Betroffenen/Daten, Beschreibung der Folgen, ergriffene/zu ergreifende (Sicherheits-) Mass nahmen

Datensicherheit / Privacy by Design & Default

Fragen	Massnahmen	Erläuterung
• Wie wird die Datensicherheit technisch gewährleistet? • Wie ist der Zugriff auf (besonders schützenswerte) Personendaten geregelt / eingeschränkt?	✓ Überprüfung Zustand und Anpassung der technischen / organisatorischen Sicherheitsmassnahmen ✓ Einführung von Security Audits ✓ Sicherstellung der Dokumentation allfälliger Sicherheitsverletzungen (vgl. oben S. 12) ✓ Prozesse für Privacy-by-Design / -Default in Organisation einführen	• Ziel: kein unbefugter / zufälliger Verlust, keine Vernichtung, keine unbefugte Zugriffe • Sicherstellung Vertraulichkeit, Verfügbarkeit und Integrität • Risikobasierter Ansatz
• Welche organisatorische Massnahmen bestehen? • Wie und ab wann wird Privacy in der Planung von Datenverarbeitungsprozessen berücksichtigt?		Die DSGVO verpflichtet Unternehmen, Datenschutz und Datensicherheit bereits beim Produktedesign zu berücksichtigen und datenschutzfreundliche Voreinstellungen zu tätigen
• Haben wir ein IT-Sicherheitskonzept, das auf einer Risikoanalyse basiert? • Wird Risikoanalyse periodisch wiederholt / dokumentiert?		Namentlich bei der Datensicherheit folgt die DSGVO einem risikobasierter Ansatz

Governance

Fragen	Massnahmen	Erläuterung
• Besteht unsere Kerntätigkeit in der Durchführung von Datenverarbeitungen, die umfangreiche, regelmässige und systematische Überwachung des Verhaltens von Personen erfordert? • Besteht unsere Kerntätigkeit in der Durchführung von Datenverarbeitungen, die umfangreiche Verarbeitung besonders geschützter Personendaten (z.B. Patientendaten) erfordert?	✓ Prüfen, ob Pflicht zur Ernennung eines Datenschutzbeauftragten besteht ✓ Ernennung des Datenschutzbeauftragten; Veröffentlichung der Kontaktdaten und Meldung an Aufsichtsbehörde ✓ Internes Datenschutz-reglement (Data Governance Policy) anpassen/erstellen ✓ Schulung von Mitarbeitern, um das Bewusstsein für Datenschutz- und Datensicherheitsfragen zu schärfen ✓ Vertreter in der EU ernennen	• Ernennung eines Daten-schutzbeauftragten nicht für alle Unternehmen erforderlich • Ernennung erforderlich, wenn eine der beiden Fragen links mit Ja beantwortet wird • In den übrigen Fällen: Ernennung eines Daten-schutzbeauftragten oder einer im Unternehmen für Datenschutzfragen zuständigen Person empfohlen
• Haben wir ein internes Datenschutzreglement? • Verstehen unsere Mitarbeiter das Datenschutzreglement und setzen sie dieses im Unternehmensalltag um?		• Unternehmen müssen gegenüber Aufsichts-behörden aufzeigen können, dass sie den Datenschutz ernst nehmen und DSGVO-Compliance umsetzen, inkl. Schulungen
• Müssen wir einen Vertreter in der EU ernennen?		• Pflicht zur Ernennung eines Vertreters in der EU für Schweizer Unternehmen, die der EU-DSGVO unterstehen

Ausblick: Gesetzesrevision in der Schweiz und EU e-Privacy Verordnung

DSGVO-Compliance

- Problem: unvollständige, z.T. komplizierte Guidelines der EU-Datenschutzaufsichtsbehörden
- Umsetzungshilfen daher «work in progress»:
  - IAB Europe (EU-DSGVO Infos/Tools): https://www.iabeurope.eu/?s=GDPR
  - IAB UK (To Do's basierend auf Infos des ICO): https://www.iabuk.net/policy/briefings/iab-uk-gdpr-checklist
- IAB Switzerland setzt sich für risikobasierte Regulierung in der Schweiz ein

E-Privacy Verordnung

- Verordnung wird die bestehende (Cookie-) Richtlinie und deren Umsetzung im Recht der Mitgliedstaaten ersetzen; gemeinsames Inkrafttreten mit DSGVO aber unrealistisch
- Auch anwendbar für Schweizer Unternehmen, die Cookies auf Geräten von Nutzern setzen (lassen), die sich in der EU befinden
- Zementiert die Anforderung, dass Cookies nur mit Einwilligung des Nutzers gesetzt werden dürfen; andere Erlaubnistatbestände gemäss DSGVO (Vertragserfüllung und berechtigte Interessen) werden übersteuert
- Parlament hat den Vorschlag der Kommission sogar noch verschärft (Erklärtes Ziel, so MEP Birgitt Sippel: «abolish surveillance driven advertising»!)
- Finale Verhandlungsphase im Gang
- Lobbying der Medien- und Werbeverbände inkl. IAB Europe

Ihr Kontakt bei VISCHER

Dr. Rolf Auf der Maur

Rechtsanwalt, Partner

ram@vischer.com

+41 58 211 34 00

Dr. Thomas Steiner, LL.M.

Rechtsanwalt, Senior Associate

tsteiner@vischer.com

+41 58 211 34 00

VISCHER: Your Team for Swiss Law

VISCHER

Herzlichen Dank.

Zürich
Schützengasse 1
CH-8021 Zürich
Tel +41 58 211 34 00
Fax +41 58 211 34 10

Basel
Aeschenvorstadt 4
CH-4010 Basel
Tel +41 58 211 33 00
Fax +41 58 211 33 10