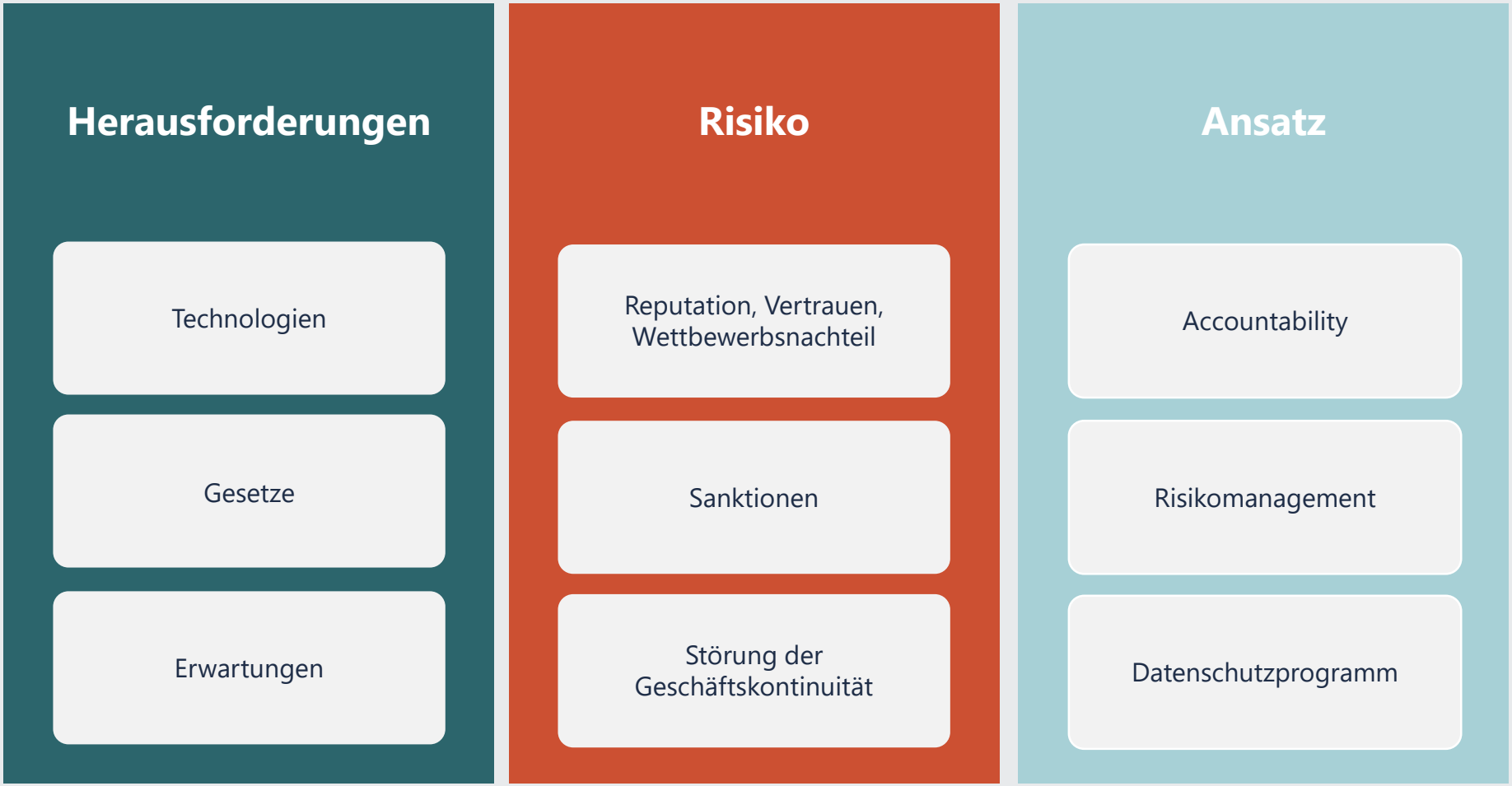
Privacy by Design: Ein neues Konzept oder Best Practice?

Daniela Fábián Masoch

Europainstitut, 12. Tagung zum Datenschutz, Zürich, 5. Februar 2019

Datenschutz ist zu einem entscheidenden Erfolgsfaktor für jedes Unternehmen geworden



Unternehmen müssen neue Herausforderungen meistern

Herausforderungen

Neue Technologien (AI, Machine Learning, Internet of Things, Big Data, Analytics, Blockchain, Cloud, Mobile Apps, etc.) eröffnen neue Möglichkeiten der Speicherung, Verarbeitung, Mobilität und Analyse von grossen Datenmengen

Gesetze (DSGVO / E-DSG) auferlegen neue Pflichten für Verantwortliche

Kunden, Mitarbeiter, Konsumenten, Patienten, Geschäftsführer und Behörden haben erhöhte Erwartungen an den Schutz ihrer Privatsphäre

Datenschutzgrundsätze sind bei der Erhebung und Verarbeitung von Personendaten zu beachten

Rechtmässigkeit / Verarbeitung nach Treu und Glauben	Jede Datenverarbeitung muss sich auf einen Rechtsgrund stützen (z.B. Vertrag, rechtliche Pflicht, berechtigtes Interesse des Verantwortlichen oder Einwilligung)
Transparenz	Betroffene Personen müssen über die Datenerhebung, den Zweck der Verarbeitung , Zugriffe u.a. informiert sein
Datenminimierung	Nur Personendaten, die für die Erfüllung des Zwecks relevant und erforderlich sind, dürfen erhoben und verarbeitet werden (so viel wie nötig – so wenig wie möglich)
Zweckbindung	Personendaten dürfen nur für die festgelegten und legitimen Zwecke verarbeitet werden (oder für Zwecke, die mit den ursprünglichen Zwecken kompatibel sind)
Vertraulichkeit	Daten müssen vertraulich behandelt und dürfen nur restriktiv an Drittpersonen (auch intern) übermittelt werden (Need-to-know Prinzip) / Einschränkung beim Datentransfer
Datenschutzrechte	Betroffene Personen müssen ihre Rechte durchsetzen können (Zugriff auf Daten, Berichtigung, Löschung, Widerspruch, Widerruf einer Einwilligung, Beschwerde, etc.)
Datenintegrität	Personendaten müssen sachlich richtig sein und gegebenenfalls berichtigt oder vernichtet werden
Datenspeicherung	Personendaten dürfen nur solange gespeichert werden, wie es für die Zweckerfüllung erforderlich ist (Ausnahmen, z.B. rechtliche Aufbewahrungspflichten)
Datensicherheit	Personendaten müssen durch technische und organisatorische Massnahmen gegen unerlaubten Zugriff, Zerstörung oder Verlust gesichert werden
Auftragsverarbeitung	Verantwortlicher muss sich vergewissern, dass Auftragsverarbeiter Datenschutz- und Sicherheitsgrundsätze gewährleisten kann und einen Vertrag abschliessen
Grenzüberschreitende Übermittlung	Personendaten dürfen nur unter bestimmten Voraussetzungen grenzüberschreitend übermittelt werden

Die Nichteinhaltung der Datenschutzgrundsätze kann zu erheblichen Risiken führen

Risiko

- Reputation, Vertrauen, Wettbewerbsnachteil
- Schwerwiegende Sanktionen und Bussen
- Störung der Geschäftskontinuität

Verantwortungsvoller Datenschutz durch Privacy by Design

Ansatz

Verantwortung für die Einhaltung des Datenschutzes übernehmen

Risiken voraussehen und proaktiv managen

Risikobasierte Strategie und Datenschutzprogramm umsetzen

Verantwortungsvoller Datenschutz heisst....

- Verantwortung übernehmen
  - Rollen und Verantwortlichkeiten im Bereich Datenschutz festlegen
  - Risiken voraussehen und managen
  - Datenschutzprogramm umsetzen
  - Kontrollen durchführen
- Datenschutz bereits in die Konzeption und Erstellung von Datenverarbeitungssystemen und Geschäftsprozessen integrieren
- Personendaten während des gesamten Lebenszyklus, von der Erhebung bis zur Vernichtung, sichern

Was ist Privacy by Design?

- Operative Umsetzung der Datenschutzgrundsätze
- Grundvoraussetzung für die effektive Umsetzung des Datenschutzes
- Verlangt, dass Verantwortliche die Datenschutzgrundsätze bereits in der Anfangsphase des Designs und während des gesamten Entwicklungsprozesses neuer Systeme, Geschäftsprozesse, Dienstleistungen oder Produkte, die die Verarbeitung personenbezogener Daten beinhalten, berücksichtigt
- Stellt Einhaltung der gesetzlichen Anforderungen und Rechenschaftspflicht sicher und erlaubt frühzeitige strategische und operative Entscheidungen, um Geschäftsprozesse und Systeme effizient zu gestalten

Accountability

- Der Verantwortliche muss bei der Verarbeitung von Personendaten die Datenschutzgrundsätze einhalten und
- die Einhaltung nachweisen können

Risikomanagement

- Der Verantwortliche muss die mit der Datenverarbeitung verbundenen Risiken für die betroffenen Personen und die Organisation voraussehen und
- Massnahmen zur Eliminierung, Reduktion oder Bewältigung der Risiken treffen

Datenschutzmanagement

- Der Verantwortliche muss technische und organisatorische Massnahmen zur effektiven Implementierung des Datenschutzes einführen
- Dokumentation der Verfahren ist die Basis für eine gute Datenschutzmanagement-Praxis

Das Konzept "Privacy by Design" als Best Practice

Das Konzept "Privacy by Design" existiert seit Jahren als Best Practice und wird in diversen Dokumenten erwähnt:

- EG 46 der EU Richtlinie 46/95 erwähnt das Konzept indirekt
- Die damalige Information and Privacy Commissioner von Ontario hat 2009 den Begriff »Privacy by Design» eingeführt und 7 Grundprinzipien definiert
- Die 32nd International Conference of Data Protection and Privacy Commissioners hat 2010 "Privacy by Design" als "*an essential component of fundamental privacy provisions*" anerkannt
- Das Konzept ist auch im Leitfaden des EDOEB zu den technischen und organisatorischen Massnahmen des Datenschutzes enthalten

Die 7 Grundprinzipien von Privacy by Design

Prinzip	Bedeutung für Verantwortliche
Be proactive not reactive; preventative not remedial	Verantwortliche sollen proaktiv datenschutzrelevante Ereignisse und Risiken voraussehen und verhindern, bevor sie eintreten (Datenschutz als Teil der Geschäftskultur integrieren)
Privacy as the Default	Verantwortliche sollen die Datenschutzgrundätze zum Schutz von Personendaten standardmässig in Ablagesysteme und Geschäftsprozesse integrieren, ohne dass die betroffenen Personen aktiv werden müssen
Privacy embedded into Design	Verantwortliche sollen die Datenschutzgrundsätze in das Design und die Architektur von IT Systemen und Geschäftsprozessen so integrieren, dass die Privatsphäre zu einem wesentlichen Bestandteil der gelieferten Kernfunktionalität wird
Full functionality – positive sum, not zero sum	Verantwortliche sollen alle berechtigten Interessen und Ziele, und nicht nur die Datenschutzziele, ohne unnötige Kompromisse berücksichtigen.
End-to-end security – lifecycle protection	Verantwortliche sollen Personendaten je nach Sensibilität während des gesamten Lebenszyklus durch technische und organisatorische Maßnahmen schützen (wie geeignete Verschlüsselung und starke Zugangskontrollen)
Visibility and transparency	Verantwortliche sollen betreffend der Verarbeitungstätigkeiten transparent sein und damit Verantwortlichkeit zeigen und Vertrauen aufbauen
Respect for User Privacy	Verantwortliche sollen die Privatsphäre der betroffenen Personen in den Mittelpunkt des Interesses stellen (Information, datenschutzfreundliche Einstellungen und Optionen)

Was ist mit der DSGVO neu?

Best Practice wird zur gesetzlichen Pflicht für Verantwortliche: Neu müssen Unternehmen Privacy by Design nachweislich umsetzen (Sanktionen nach Art. 83 DSGVO)

- Art. 25 DSGVO
  - Data protection by design and by default
  - Protection des données dès la conception et protection des données par défaut
  - Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita
  - Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellung
- Art. 6 E-DSG
  - Data protection by design and by default
  - Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

Was sagt Art. 25 DSGVO?

Art. 25 DSGVO umschreibt das Konzept Privacy by Design:

Wer ist verpflichtet?	Der Verantwortliche (Hersteller von Produkten, Dienstleistungen und Anwendungen wird ermutigt PbD zu berücksichtigen – EG 78)
Was muss getan werden?	Technische und organisatorische Massnahmen (TOMs) müssen getroffen werden (Beispiel: Pseudonymisierung)
Wie müssen TOMs sein?	- Angemessen • Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, Umfang, Umstände und Zwecke der Verarbeitung sowie Risiken für die betroffenen Personen - Geeignet, die Datenschutzgrundsätze (Beispiel: Datenminimierung) wirksam umzusetzen und die Rechte der betroffenen Personen zu schützen
Wann müssen TOMs getroffen werden?	Sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch während der eigentlichen Verarbeitung

Pseudonymisierung ist nur eine der möglichen TOMs

- Art. 25 DSGVO erwähnt die Pseudonymisierung als Beispiel für eine geeignete TOM
- Weitere technische und organisatorische Massnahmen müssen ebenfalls berücksichtigt werden:
  - Technische Massnahmen, wie:
    - Zugriffsberechtigungen- und Einschränkungen
    - Nutzerauthentifizierung
    - Zugangsbeschränkungen
    - Verschlüsselung
    - Protokollierungen
    - Physische Schutzmassnahmen
    - Technische Umsetzung des Widerspruchsrechts, Korrektur, Löschung oder Daten Portabilität
  - Organisatorische Massnahmen, wie:
    - Erstellung und Umsetzung von Policies, Reglementen, Weisungen, Anleitungen und Handbücher
    - Dokumentation der Verarbeitungstätigkeiten (Inventar), Datenpannen sowie Datenschutzfolgeabschätzungen
    - Assessment von und Verträge mit Dienstleistern
    - Schulungen
    - Kontrollen

Datenminimierung ist nur eines der Datenschutzgrundsätze die es zu beachten gilt

- Art. 25 DSGVO erwähnt die Datenminimierung als eines der Datenschutzgrundsätze, die durch die TOMs wirksam umgesetzt werden sollen
- Weitere Datenschutzgrundsätze sind bei der Verarbeitung von Personendaten ebenfalls zu berücksichtigen, wie:
  - Rechtmässigkeit
  - Transparenz
  - Vertraulichkeit
  - Zweckbindung
  - Datenintegrität
  - Speicherdauer
  - Sicherheit
  - Sichere Auftragsdatenverarbeitung
  - Sichere und legitime grenzüberschreitende Datenübermittlung
  - Wahrung der Rechte der betroffenen Personen

Wie kann Privacy by Design umgesetzt werden?

- Art. 25 DSGVO sagt nicht, wie Privacy by Design konkret umgesetzt werden soll
- Ein Ansatz ist die Implementierung eines Risiko- und Datenschutzmanagementprogramms mit folgenden Elementen:

Prozessbeschreibungen für die konkrete Umsetzung von Privacy by Design

Konformitätsprüfung, Risikobeurteilung und Festlegung der erforderlichen Massnahmen

Die Konformitätsprüfung und Risikobeurteilung, ggf. DSFA, beantwortet Fragen wie:

- Ist der Bearbeitungszweck konkret umschrieben? Wie wird sichergestellt, dass die Daten nicht für andere Zwecke verarbeitet werden?
- Besteht eine rechtliche Grundlage für die Verarbeitung der Personendaten? Ist eine Einwilligung erforderlich und, falls ja, wie soll diese eingeholt und dokumentiert werden? Falls ein berechtigtes Interesse des Verantwortlichen besteht, ist eine Abwägung der Interessen vorgenommen und dokumentiert worden?
- Sind alle vorgesehenen Personendaten erforderlich um den Zweck zu erfüllen oder kann ggf. auf gewisse Datensätze verzichtet werden? Kann der Zweck auch mit anonymen oder pseudonymen Daten erfüllt werden?
- Sind die Systeme, Websites, Apps, Geschäftsprozesse und Produkte, welche Personendaten speichern oder verarbeiten so aufgesetzt, dass nur die erforderlichen Personendaten für den jeweiligen Zweck gespeichert und verarbeitet werden? Wie wird sichergestellt, dass die Daten nicht für andere Zwecke verarbeitet werden?
- Wer soll Zugriff auf welche Personendaten haben und zu welchem Zweck? Sind allfällige Auftragsverarbeiter geprüft worden um sicherzustellen, dass diese in der Lage sind, die datenschutzrechtlichen Anforderungen zu erfüllen?
- Bestehen angemessene Verträge mit Auftragsverarbeiter und weiteren Personen, die Personendaten zur Verarbeitung erhalten?

Konformitätsprüfung, Risikobeurteilung und Festlegung der erforderlichen Massnahmen (Forts.)

- Ist der Personenkreis, der Zugriff auf die Personendaten oder einzelne Datensätze haben soll, definiert und dokumentiert? Wie wird der Zugriff kontrolliert und eingeschränkt?
- Wird ggf. aus dem Ausland auf die Personendaten zugegriffen oder werden Daten ins Ausland transferiert? Falls ja, bestehen geeignete Garantien um den Datentransfer zu legitimieren? Wie werden die Garantien umgesetzt und die Einhaltung kontrolliert?
- Welche Rechte haben die betroffenen Personen? Gibt es ggf. Einschränkungen? Wie wird sichergestellt, dass die Rechte effektiv ausgeübt werden können? Wer ist für Anfragen verantwortlich? Wie werden Rechte wie Daten Portabilität, Löschung, Widerruf der Einwilligung, etc. gewährleistet?
- Wie lange sollen die Personendaten gespeichert und verarbeitet werden? Liegt ein Retentions- und Löschkonzept vor?
- Sind die betroffenen Personen über die Verarbeitung ihrer Personendaten informiert, bzw. ist eine Information vorgesehen und wie soll diese durchgeführt werden? Ist die Information verständlich geschrieben?
- Sind angemessene datenschutzfreundliche technische Massnahmen geplant? Wenn ja, welche und wie werden diese umgesetzt?
- Welche Sicherheitsmassnahmen werden getroffen um Sicherheitsvorfälle zu vermeiden? Wie ist der Prozess im Falle eines Sicherheitsvorfalls?
- Sind die Verantwortlichkeiten für die Umsetzung, die Verifizierung und die Durchführung von periodischen Kontrollen der Massnahmen festgelegt?

Beispiel: Privacy by Design für Mobile Apps

Beispiel	Relevante Fragen	Mögliche Massnahmen
Mobile App:	• Funktionalitäten der App.?	
	• Involvierte Parteien, Rollen, Zugriffe und Verantwortlichkeiten?	• Zugriffsrechte und -einschränkungen regeln und sicherstellen
	• Erforderliche Daten, je nach Funktionalität der App. (Registrierung, Nutzung, Ortung, Inhalt) – Pseudonyme / anonyme / weniger Daten? Wie wird sichergestellt, dass nicht mehr Daten gespeichert werden?	• Datenminimierung durch entsprechende Einstellungen
	• Zweck der Datenverarbeitung und Rechtsgrundlage? Anforderungen an die Einwilligung? Wie wird die Zweckbindung sichergestellt?	• Betriebshandbuch / Weisungen / Dokumentation / Schulungen • Prozess bei Widerruf der Einwilligung
	• Dauer, Zweck und Ort der Datenspeicherung?	• Retentions- und Löschkonzept, Anonymisierungsprozess
	• Ausübung der Datenschutzrechte (welche und wie)?	• Prozess und technische Maßnahmen und Automatismen (Such- und Löschfunktionen, Selbstmanagement (De-Aktvierung) durch Nutzer)
	• Wie werden die Daten vor unberechtigtem Zugriff, Verlust, Diebstahl oder Änderung gesichert?	• Pseudonymisierung, Verschlüsselung, Segregieren, Back-up, etc. • Prozess bei Datenpannen
	• Verarbeitung durch Dritte?	• Due Diligence Prozess für Auftragsverarbeiter, Verträge und Audits
	• Übermittlung ins / Zugriff aus dem Ausland	• Garantien für grenzüberschreitende Datentransfers
	• Wie und wann werden die betroffenen Personen informiert?	• Information über die Erhebung, Zweck, Verarbeitung und Zugriff der Daten vor dem Download oder Aktivierung der App und bei jeder Änderung

Beispiel: Privacy by Design für CRM Systeme

Beispiel	Relevante Fragen	Mögliche Massnahmen
Globales CRM System	Funktionalitäten des Systems: Adress- und Kontaktverwaltung; Protokollierung von Geschäftsbeziehungen; Marketingaktivitäten (Einladungen, Newsletters, Geburtstagskarten), Aufgabenplanung, etc.	
	Involvierte Parteien, Rollen und Verantwortlichkeiten, Dienstleister, Datensubjekte?	Zugriffsrechte und -einschränkungen regeln und sicherstellen
	Erforderliche Daten, je nach Funktionalität und Zweck der Verarbeitung (Stammdaten, weitere Informationen, Social Media, Profiling?) – Freie Felder?	Datenminimierung durch entsprechende Einstellungen, freie Felder deaktivieren oder Nutzer entsprechend schulen
	Quelle der Daten (direkt, indirekt)	Entsprechend informieren
	Rechtsgrundlage für jede Verarbeitung? Einwilligung?	Ggf. berechtigtes Interesse und Einwilligung dokumentieren und managen (Abwägung, Widerruf)
	Dauer, Zweck und Ort der Datenspeicherung?	Retentions- und Löschkonzept, Anonymisierungsprozesse
	Wie wird die Datenqualität sichergestellt?	Regelmäßige Überprüfungen, Self-management?
	Ausübung der Datenschutzrechte?	Technische Massnahmen, Automatismen, Verantwortlichkeiten, Such- und Löschfunktinen, Self-Management?
	Sicherheit und Schutz der Daten vor unberechtigten Zugriff, Verlust, Diebstahl, Veränderung, etc.	TOMs, Pseudonymisierung, Verschlüsselung, Segregieren, Back-up,
	Verarbeitung durch Dritte?	Due Diligence Prozess für Auftragsverarbeiter, Verträge und Audits
	Übermittlung ins / Zugriff aus dem Ausland	Garantien für grenzüberschreitende Datentransfers

Privacy by Design – ein neues Konzept oder Best Practice?

- Das Konzept «Privacy by Design» ist nicht neu und gilt seit Jahren als Best Practice
- Neu ist die Aufnahme des Konzepts in die DSGVO als rechtliche Verpflichtung für Verantwortliche
- Privacy by Design ist eine Grundvoraussetzung um Datenschutz effektiv und nachhaltig umzusetzen und die Basis für ein gut funktionierendes Datenschutzmanagementprogramm
- Implementierung von Privacy by Design ist eine Teamarbeit zwischen Business, Informationssicherheit / IT und Legal / Datenschutz

Fragen?

FABIAN PRIVACY LEGAL GmbH
Daniela Fábián Masoch
Bäumleingasse 10
4051 Basel
daniela.fabian@privacylegal.ch
www.privacylegal.ch