NEUES ZUM CCPA UND ZUM DATENTRANSFER IN DIE USA

Datenschutz am Mittag

14. März 2023

Agenda

Teil I – Axel Spies

- Datenschutz in den USA – gibt es nicht?
- Vorreiter Kalifornien: Der reformierte CCPA
- Vergleich mit anderen Bundesstaaten
- Ausblick

Teil II – Barbara Schmitz

- Datentransfer in die USA
- Ausblick

Q&A

Teil I – Datenschutz in den USA

Morgan Lewis

Datenschutz in den USA – gibt es nicht?

Morgan Lewis

System des Datenschutzes in den USA

- Keine allumfassende Regelung wie DS-GVO, sondern Mischung aus:
- Sektorspezifische Regelungen, zum Beispiel:
  - Gesundheitssektor
  - Finanzsektor
- Spezialgesetze, zum Beispiel:
  - Regelungen für Bruch der Datensicherheit: keine bundesgesetzliche Regelung, aber alle Bundesstaaten haben entsprechende Vorschriften erlassen
  - Regelungen für Online-Daten
  - CPNI der FCC: Schutz der Daten die von Konsumenten an Netzbetreiber übergeben warden (customer proprietary network information)
    - ➢ Jährliche Zertifizierung notwendig

System des Datenschutzes in den USA

- American Data Privacy Protection Act (ADPPA) als bundesgesetzliche, sektorübergreifende Regelung
  - Entwurf im zuständigen Ausschuss des Repräsentantenhauses gebilligt (Juli 2022)
  - Auswirkungen der Zwischenwahlen noch nicht absehbar (Nov. 2022)
- Bundesstaaten haben teilweise eigene sektorübergreifende Datenschutzgesetze
  - Kalifornien als Vorreiter mit CCPA (seit 1.1.2020) und CPRA (seit 1.1.2023)
  - Virginia (seit 1.1.2023)
  - Colorado (ab 1.7.2023)
  - Connecticut (ab 1.7.2023)
  - Utah (ab 31.12.2023)

Vorreiter Kalifornien: Der reformierte CCPA

Morgan Lewis

CCPA

- California Consumer Privacy Act (CCPA)
- Inkraft seit 1.1.2020
- Umfasst Rechte für den Schutz der Privatsphäre von Verbrauchern (= auch Angestellte und Einzelpersonen, die in einem kommerziellen Kontext handeln)
- Verpflichtungen für Unternehmen in Bezug auf die Erhebung und den „*Sale*" von personenbezogenen Daten
- Schwellenwert:
  - Bruttojahresumsatz von mind. $ 25 Mio. *oder*
  - Verarbeitung der persönlichen Daten von mind. 100.000 Gebietsansässigen *oder*
  - Erzielung von 50 % oder mehr des Jahresumsatzes aus dem Verkauf (sell, buy, receive oder *share*) personenbezogener Daten von Einwohnern Kaliforniens
- Außerdem: California Data Broker Law

Achtung: *Sale* unter dem CCPA

Breite Definition in Section 1798.140(ad)(1) – Sale =

- Verkauf,
- Vermietung,
- Freigabe,
- Offenlegung,
- Verbreitung,
- Zurverfügungstellung,
- Übertragung oder
- anderweitige mündliche, schriftliche, elektronische oder sonstige Übermittlung der personenbezogenen Daten eines Verbrauchers durch das Unternehmen

an einen Dritten gegen Geld oder eine andere entgeltliche Gegenleistung.

CPRA oder CCPA 2.0

- California Consumer Privacy Rights Act (CPRA)
  - Ergänzung zum CCPA
  - In Kraft seit 1.1.2023
- Schaffung der California Privacy Protection Agency als Datenschutzbehörde
  - Beginn mit Durchsetzung von Geldbußen bereits im Feb. 2023
- Weitere Änderungen:
  - Abschaffung der Gnadenfrist, innerhalb derer Verstöße ohne Strafe behoben werden konnten
  - Verbot, Daten länger als nötig aufzubewahren

Implementierungsvorschrift in Bezug auf die Datenschutzerklärung (seit 3.2.2023)

Teil 1: Information über gesammelte Daten

- Kategorien von erfassten personenbezogenen Daten sowie Benennung der Kategorien der Quellen dieser Daten,
- Geschäftliche Zwecke der Sammlung von personenbezogenen Daten,
- Kategorien von personenbezogenen Daten, die „verkauft" (definiert im CCPA) oder sonst wie an Dritte weitergeleitet werden sowie Kategorisierung der Dritten, an die diese Daten weitergegeben werden,
- Eine Erklärung darüber, ob das Unternehmen tatsächlich Kenntnis davon hat, dass es personenbezogene Daten von Verbrauchern unter 16 Jahren verkauft oder weitergibt,
- Eine Erklärung darüber, ob personenbezogene Daten gegenüber Dritten in den letzten 12 Monaten offengelegt wurden – wenn ja, dann müssen die Dritten in Kategorien eingeteilt werden und der spezifische geschäftliche Zweck dieser Offenlegung benannt werden.

Implementierungsvorschrift in Bezug auf die Datenschutzerklärung (seit 3.2.2023)

Teil 2: Aufklärung über Rechte

- Recht auf Auskunft
- Recht auf Löschung,
- Recht auf Datenberichtigung,
- Recht auf Opt-out von Verkauf und Weitergabe der personenbezogenen Daten,
- Recht auf Begrenzung der Nutzung von sensiblen personenbezogenen Daten, wenn solche verarbeitet werden
- Recht auf Diskriminierungsfreiheit, wenn von den Rechten Gebrauch gemacht wird

Teil 3: Information über Verfahren

- Benennung der Ausübungsmethoden
- Anleitung für Stellung einer Anfrage (inkl. Link zu Formular / Portal)
- Belehrung über Opt-Out bei „Verkauf" oder Weitergabe von personenbezogenen Daten
- Beschreibung des internen Prozesses bei Anfragen
- Erklärung darüber, wie eine Opt-out Anfrage verarbeitet und unverzüglich umgesetzt wird

Implementierungsvorschrift in Bezug auf die Datenschutzerklärung (seit 3.2.2023)

- Bei Online-Datenerhebung:
  - Link direkt an die Stelle der Datenschutzerklärung, an der die Informationen aufgelistet sind
  - Link lediglich an den Beginn der Erklärung ist nicht ausreichend
- Bei Teilen / „Verkauf" der Daten an Dritten:
  - Belehrung über Recht zum Opt-Out
  - Link für Widerspruch muss vorhanden sein (spezifische Anforderungen, wann und wie dieser Link angezeigt werden muss)

Weitere Implementierungsvorschriften in Planung

- Öffentliche Anhörung zu geplanter Regelung im Gange (bis 27. März)
- Jährlicher Cybersecurity-Audit durch neue Datenschutzbehörde
- Zusätzlich: Risikobewertung muss von Unternehmen abgegeben werden

Vergleich mit anderen Bundesstaaten

Morgan Lewis

Rechte der Betroffenen

US-Bundesstaat	Kalifornien (CPRA)	Kalifornien (CPPA)	Colorado Privacy Act	Utah Consumer Privacy Act	Virginia Consumer Data Protection Act
Inkrafttreten	1.1.2023	1.1.2020	1.7.2023	31.12.2023	1.7.2023
Recht auf Datenzugang	X	X	X	X	X
Recht auf Berichtigung	X		X		X
Recht auf Löschung	X	X	X	X	X
Recht auf Verarbeitungsbeschränkung	X			X	X
Recht auf Portabilität	X	X	X		X
Recht auf Opt-out	X	X	X	X beschränkt	X
Private Right of Action	X	X			
Recht gegen automatisierte Entscheidungstreffung	X		X		X
Allgemeines Private Right of Action – Klagerecht	X	X			
Recht auf Anfechtung einer Entscheidung, die den Datenzugang (Access Request) versagt.			X		X

Anforderungen an den Verarbeiter

US-Bundesstaat	Kalifornien (CPRA)	Kalifornien (CPPA)	Colorado Privacy Act	Utah Consumer Privacy Act	Virginia Consumer Data Protection Act
Inkrafttreten	1.1.2023	1.1.2020	1.7.2023	31.12.2023	1.7.2023
Privacy Notice - Transparenzerfordernis	X	X	X	X	X
Benachrichtigungspflicht bei einem Bruch der Datensicherheit					
Impact Assessments geregelt oder erforderlich	X		X		X
Diskriminierungsverbot bei der Ausübung der Rechte	X	X	X	X	X
Zweckbegrenzung bei der Verarbeitung	X	X	X	X	X
Data Processing Agreements erforderlich	X	X	X	X	X
Zweckbegrenzung	X	X	X		X
Korrekturfrist bei Verstößen			X (60 Tage)	X (30 Tage)	X (30 Tage)
Pflicht zur Datenminimisierung	X		X	X	X
Besondere Regelungen für sensitive Daten	X		X		X

Datenschutz und Datenminimierung

US-Bundesstaat	Kalifornien (CPRA)	Kalifornien (CPPA)	Colorado Privacy Act	Utah Consumer Privacy Act	Virginia Consumer Data Protection Act
Inkrafttreten	1.1.2023	1.1.2020	1.7.2023	31.12.2023	1.7.2023
Überwachung der Implementierung (Data Protection Program)	X	X	X	X	X
Regelungen zur Datenlöschung					
Reguliert „Sale" der Daten	Opt-out		X		X
Notifizierungspflichten bei Bruch der Datensicherheit	X	X	X	X	X
Überwachung der Implementierung (Data Protection Program)	X	X	X	X	X

Pflichten gegenüber Dritten und biometrische Daten

US-Bundesstaat	Kalifornien (CPRA)	Kalifornien (CPPA)	Colorado Privacy Act	Utah Consumer Privacy Act	Virginia Consumer Data Protection Act
Inkrafttreten	1.1.2023	1.1.2020	1.7.2023	31.12.2023	1.7.2023
Pflichten für Dienstleister - Service Providers (SP)	X		X	X	X
Datenschutzprogramm für Third-Party SP			X		X
Reguliert die Sammlung und/oder Speicherung	X	X	X	X	X

Illinois: Biometric Information Privacy Act (BIPA)

- Anforderung an Unternehmen (häufig ArbG): ausdrückliche Zustimmung, bevor biometrische Daten einer Person erhoben oder verarbeitet werden
- Anwendung: Fingerabdruck-, Netzhaut- oder Gesichtserkennungstechnologie
  - zB bei Eingangskontrolle, Zeiterfassung
- Verstoß gegen BIPA: jeder neue Scan biometrischer Daten bzw. jede Übermittlung an Dritte lässt Schadensersatzansprüche entstehen
  - $ 1.000 bei fahrlässigem Verstoß
  - $ 5.000 bei vorsätzlichem / grob fahrlässigem Verstoß
- 2022: Verfahren mit Schadensersatz in Höhe von $ 228 Mio. (*Richard Rogers v. BNSF Railway Company*)

Ausblick

Andere Bundesstaaten

- In vielen anderen Bundesstaaten befindet sich ein Datenschutzgesetz im Gesetzgebungsprozess
- Diese unterscheiden sich:
  - Rechte der Verbraucher (zB Opt-Out für sensible persönliche Daten möglich?)
  - Pflichten für Unternehmen (zB Risikobewertung notwendig?)

Bundesstaaten mit Datenschutzgesetzen im Gesetzgebungsprozess

- Hawaii
- Illinois
- Iowa
- Indiana
- Kentucky
- Maryland
- Massachusetts
- Minnesota
- Montana
- New Hampshire
- New Jersey
- New York
- Oklahoma
- Oregon
- Tennessee
- Texas
- Vermont
- Washington
- West Virginia

Herausforderungen für europäische Unternehmen

- Teilweise starke Abweichungen von der DS-GVO
- Schwellenwerte unterschiedlich
- Inhaltsvorgaben für Datenschutzerklärung abweichend
- Unterschiedliche Definitionen in den einzlnen Bundesstaaten

- Es gibt keinen „Goldstandard", DS-GVO Dokumente dürfen keinesfalls ungeprüft übernommen werden
- Unterschiedliche Opt-In / Opt-Out Regelungen in den Bundesstaaten

Was müssen europäische Unternehmen nun machen?

- Genaue Prüfung, ob Datenschutzrechte der verschiedenen Bundesstaaten auf ihr Geschäft anwendbar sind (Kunden? Mitarbeiter in Kalifornien? Schwellenwerte?)
- Überarbeitung und Anpassung bestehender Datenschutzerklärungen
- Prüfung von Verträgen mit Dritten
- Überprüfung und Anpassung von Websites (Opt-Out Button, Links …)
- Überprüfung interner Prozesse (Antwortfristen, teilw. Darstellung der Prozesse in der Datenschutzerklärung notwendig)
- Kalifornien (CPRA): Arbeitnehmer auch vom Anwendungsbereich umfasst
  - Umfassende Information über Datensammlung / -verwendung / -weitergabe notwendig
  - Berücksichtigung von neuen Rechten für Arbeitnehmer

Teil II – Datentransfer in die USA

Timeline aus europäischer Sicht

- ✓ Vorschlag der EU-Kommission vom 13.12.2022
- ✓ Stellungnahme LIBE vom 14.02.2023
- ✓ Stellungnahme EDSA/EDPB vom 28.02.2023
- ⌛ Stellungnahme des Ausschusses nach Artikel 93 DS-GVO die von einer qualifizierten Mehrheit der Mitgliedstaaten abgegeben wird
- ⌛ Annahme der Entscheidung durch das Kollegium der Kommissionsmitglieder

Sommer 2023 (Didier Reynders am 12.12.22 Politico/CIPL Talk ab Minute 32:25)

Will it stay or will it go?

- 29.11.2022 - HmbBfDI
- 12.12.2022 - Didier Reynders Politico/CIPL Talk
- 14.12.2022 - Wissenschaftliche Dienst EPRS
- 13.12.2022 - NOYB (Schrems)

What Shall We Do Now?

Standardvertragsklauseln nutzen

EU-US-DPF Verfahren = Beurteilungselement für Klausel 14 Abs. b) ii) iVm Fn. 12 der SCC :

- ✓ „Gepflogenheiten" des Drittlandes
- ✓ „fortlaufend mit gebührender Sorgfalt erstellt und von leitender Ebene bestätigt wurden"

Bruno Gencarelli, Leiter Bereich International Data Flows Europäischen-Komm nach der Veröffentlichung des Entwurfs EU-US-DPF:

"*The safeguards we negotiated governing [US government] access – the safeguards on necessity, proportionality, requests – have been negotiated so that they will be effective . . . and they will apply to any transatlantic transfer regardless of the mechanism used, including transfers on the basis of standard contractual clauses or binding corporate rules*."

Anything else?!

Marktortprinzip – Importeuer unterliegt bereits der DS-GVO

- Art. 3 DS-GVO – Art. 1 Durchführungsbeschluss SCC – Art. 50 DS-GVO
- a.A. EDPB Guidelines 05/2021 v 14.2.2023: „neues Set an SCC für Importeure located in 3rd country"

WTO Joint Initiative – Vorschlag der EU v. 26.4.2019 (INF/ECOM/22 (19-2880)):

2.7 Cross-Border Data Flows

1. *Members are committed to ensuring cross-border data flows to facilitate trade in the digital economy. To that end, cross-border data flows shall not be restricted by:*

   (d) making the cross-border transfer of data contingent upon use of computing facilities or network elements in the member's territory or upon localization requirements in the Member's territory.

Anything else?!

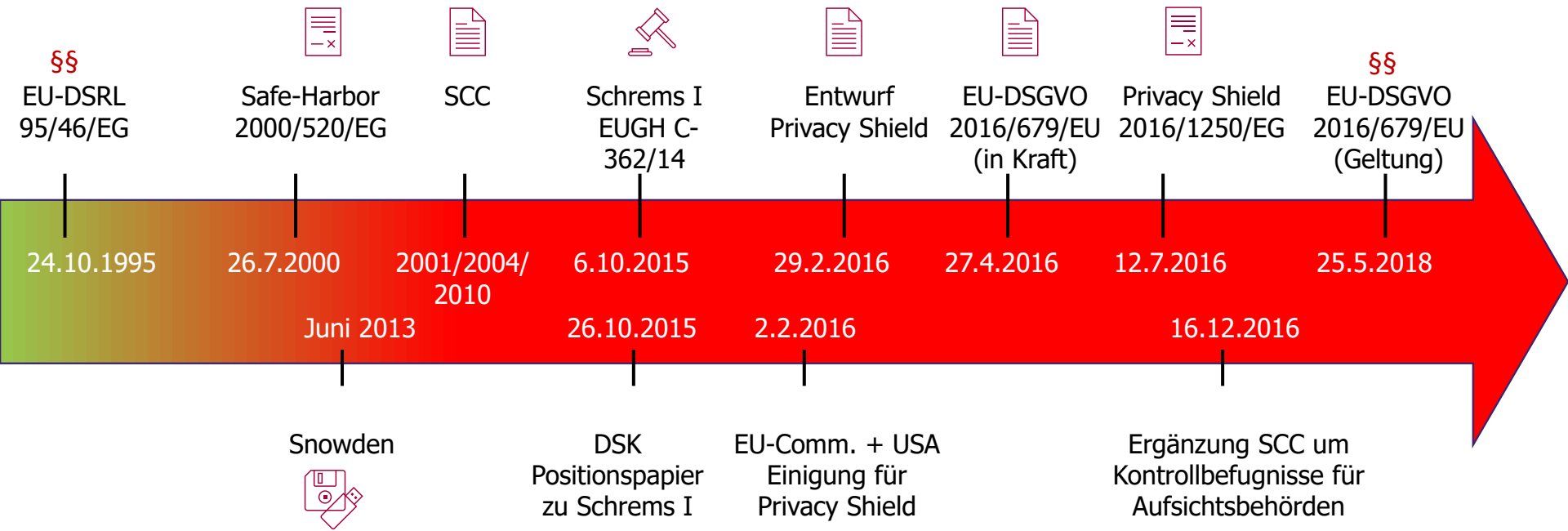
DSK-Beschluss vom 31.1.2023:

Normen und Praxis im Drittland bergen abstrakte Gefahr für unzulässige Datenübermittlung

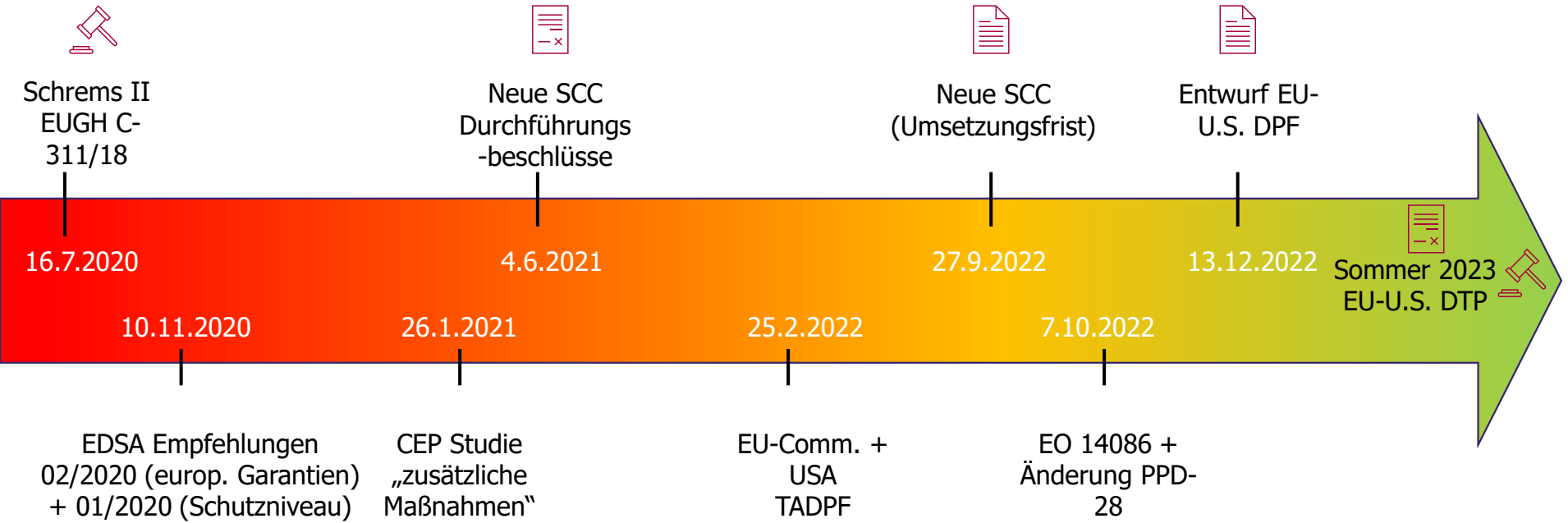
Vergabekammersache - Rechtmittelgericht

Seite 36: Ein Angemessenheitsbeschluss könnte (…) eine weisungswidrige Datenherausgabe (…) ohnehin nicht legitimieren.

Once upon a time … 1995 bis 2018



… the Story goes on: 2020 bis 2023



Q&A

Biographie

Barbara Schmitz
München
+49 89 218 390 57
Barbara.Schmitz@swmh.de

Barbara Schmitz ist Syndikusanwältin und Rechtsanwältin in München. Sie verfügt über mehr als 20 Jahre Erfahrung auf dem Gebiet des Datenschutzes in verschiedenen Unternehmen. Zunächst in der Telekommunikationsbranche, dann in der Lichtbranche und seit Januar 2021 als Syndikusrechtsanwältin für Datenschutz- und IT-Recht bei der SWMH Service GmbH. Frau Schmitz studierte Wirtschaftswissenschaften in Duisburg und Rechtswissenschaften in Münster und Bonn. Sie ist als Dozentin und Referentin auf Fachtagungen und Fortbildungsveranstaltungen aktiv und publiziert regelmäßig in Fachzeitschriften. Darüber hinaus ist sie Mitautorin verschiedener Fachkommentare. Frau Schmitz ist Mitglied des wissenschaftlichen Beirats der Zeitschrift für Datenschutz (ZD).

Biographie

Dr. Axel Spies
Washington, D.C.
+1.202.0739.6145
axel.spies@morganlewis.com

Rechtsanwalt Dr. Axel Spies studierte Rechts- und Politikwissenschaften in Bonn, Washington DC (American University) und Paris (Institut des Études Politiques). Er war nach seiner Referendarzeit in Deutschland, Russland und Indien und deutscher Promotion von 1993 bis 1994 zunächst als deutscher Rechtsanwalt im Moskauer Büro einer deutschen Kanzlei tätig. Anschließend arbeitete er fünf Jahre lang in der Rechtsabteilung der VEBA AG, Düsseldorf, zuletzt als Abteilungsleiter Öffentliches Recht.

Seit 1999 ist Dr. Spies als deutscher und europäischer Anwalt in Washington DC ansässig - zunächst für die US-Kanzlei Swidler Berlin, nach Fusionen für die US-Kanzlei Bingham McCutchen und seit Ende 2014 für Morgan, Lewis & Bockius.

Dr. Spies ist dort verantwortlich für das „German Desk" - insbesondere für die Telecommunications Media and Technology Group (TMT). Dr. Spies ist seit Jahren Mitherausgeber der deutschen Zeitschrift Multimediarecht (MMR) und deren Korrespondent in Washington. Seit Gründung der Zeitschrift für Datenschutz 2010 ist er auch deren Mitherausgeber.

DANKE