Kritis 2.0: Was gibt es nun zu beachten?

9. November 2022

Dr. Karla Klasen

Osborne Clarke Deutschland

Standorte

- Berlin, Hamburg, Köln, München

Mitarbeiter

- 450+ Mitarbeiter
- davon 200+ Rechtsanwälte und Steuerberater
- davon 64 Partner

Praxisgruppen

- Capital Markets / Banking
- Commercial / Competition
- Corporate
- Employment
- IP
- IT
- Property
- Tax

Branchenfokus

- Energy & Utilities
- Financial Services
- Life Sciences & Healthcare
- Real Estate & Infrastructure
- Retail & Consumer
- Tech, Media and Comms
- Transport & Automotive

Laufende Rechtsberatung im Sektor Energy & Utilities

Wir unterstützen Sie in allen relevanten Rechtsbereichen:

Energierecht

- Regulierung
- Netzanschluss und -nutzung
- Direktvermarktung
- Regelenergie-märkte, VK
- Projektverträge, O&M, EPC
- Repowering, Weiterbetrieb
- Eigen- und Direktverbrauch
- KAGB-/ZAG-Strukturierung

Gesellschafts-recht und Finanzierung

- Mergers & Acquisitions
- Joint Ventures, Kooperationen
- Restrukturierung
- Kapitalanlage-recht und Fonds
- Finanzaufsichts-recht
- Crowdfunding
- Projektfinanzierung
- Gesellschafts-gründungen; allg. Gesellschaftsrecht

Öffentliches Recht

- Umwelt- und Planungsrecht
- Baurecht
- Immissions-schutzrecht
- Genehmigungs-verfahren
- Widerspruchs-verfahren
- Klageverfahren

Prozess-führung

- Komplexe Zivilprozesse
- Schiedsverfahren/ Investitionsschieds-gerichtsbarkeit
- Alternative Dispute Resolution
- Insolvenzverfahren
- Gewährleistungs- und Garantie-ansprüche
- Besondere Miss-brauchsverfahren
- Clearingstelle EEG

Kartellrecht

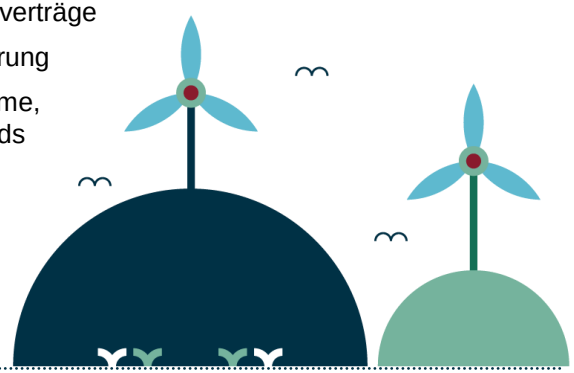
- Fusionskontrolle
- Compliance-Beratung
- Vertriebskartell-recht
- Begleitung bei Ausschreibungs-verfahren
- Konzessions-verfahren
- Rekommunali-sierung
- Zugang zu Herstellerdaten

Handel und Vertrieb

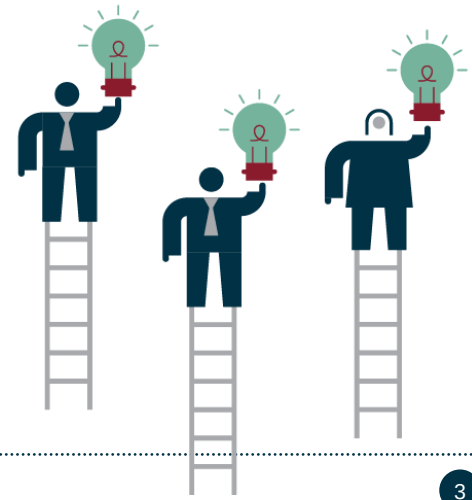
- Brennstoff- und Energiebezugs- und -lieferverträge
- Energie- und Zertifikatehandel
- Preisanpassungs-verhandlungen und -verfahren
- Handels- und Kooperations-verträge
- Vertriebssysteme
- Absatz- und Ver-triebsoptimierung

IT-Recht

- IT-Sicherheit / KRITIS
- IT-Outsourcing
- Datenschutz
- Lizenzverträge
- Forschungs- & Entwicklungs-verträge
- IT-Projektverträge
- Digitalisierung
- Smart Home, Smart Grids

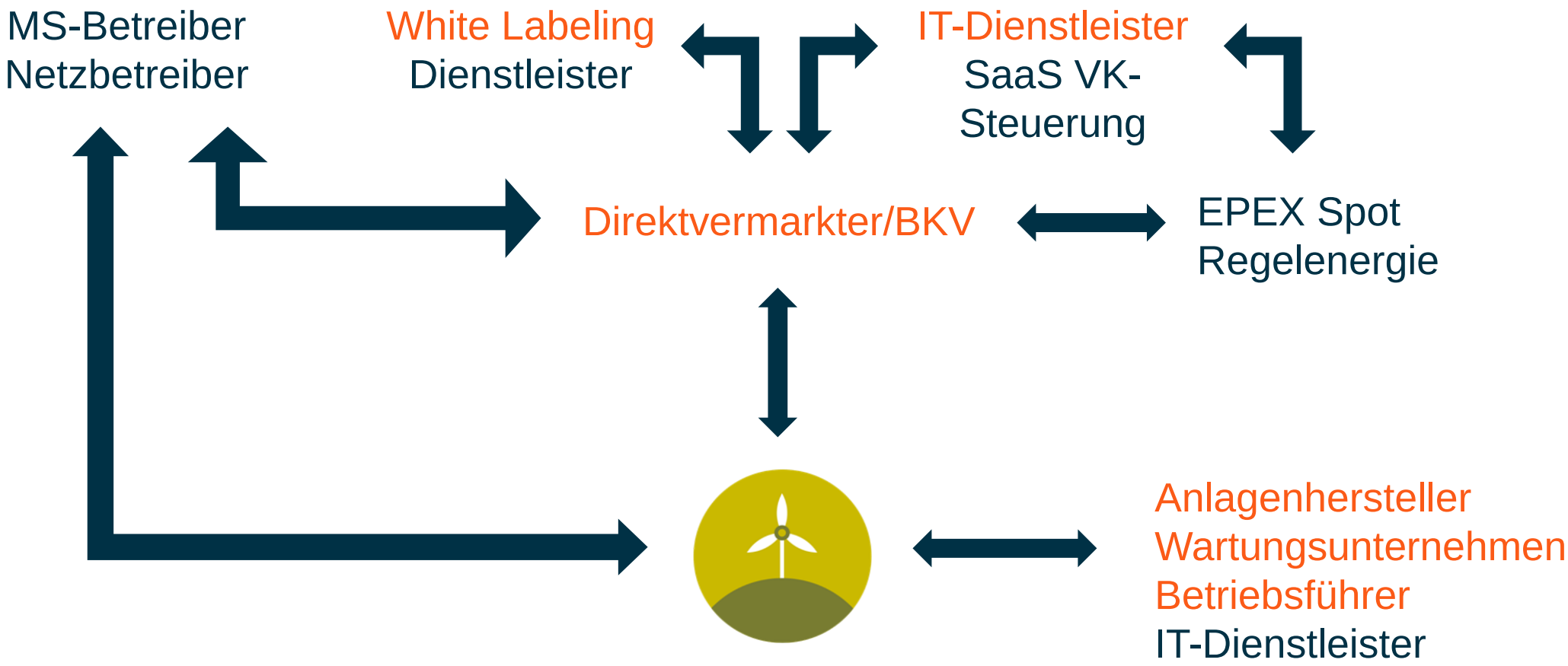


Inhalt



#1 Schnittstellen einer Windenergieanlage

(Kritische) Schnittstellen der Informationssicherheit am Beispiel der VK-Integration einer Windenergieanlage



#2 Was regeln IT-Sicherheitsgesetz, BSIG und KritisV?

Ziele des IT-Sicherheitsgesetzes

Ziele	• Verbesserung der Sicherheit informationstechnischer Systeme Kritischer Infrastrukturen in Deutschland • Besserer Schutz der Bürger im Internet • Stärkung des Bundesamts für Sicherheit in der Informationstechnik (BSI) und des Bundeskriminalamtes (BKA)
Schutzzweck	• Sicherung von Gemeinwohlinteressen im Bereich der Daseinsvorsorge, Vorgabe für entsprechende Betreiberpflichten privater Unternehmen • Vermeidung erheblicher Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse
Artikelgesetz	• Bestehende Gesetze werden geändert (insbesondere BSI-Gesetz, Telemedien- und Telekommunikationsgesetz, Energiewirtschaftsgesetz) ➢ **Das IT-Sicherheitsgesetz ist nicht direkt anwendbar**

Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG)

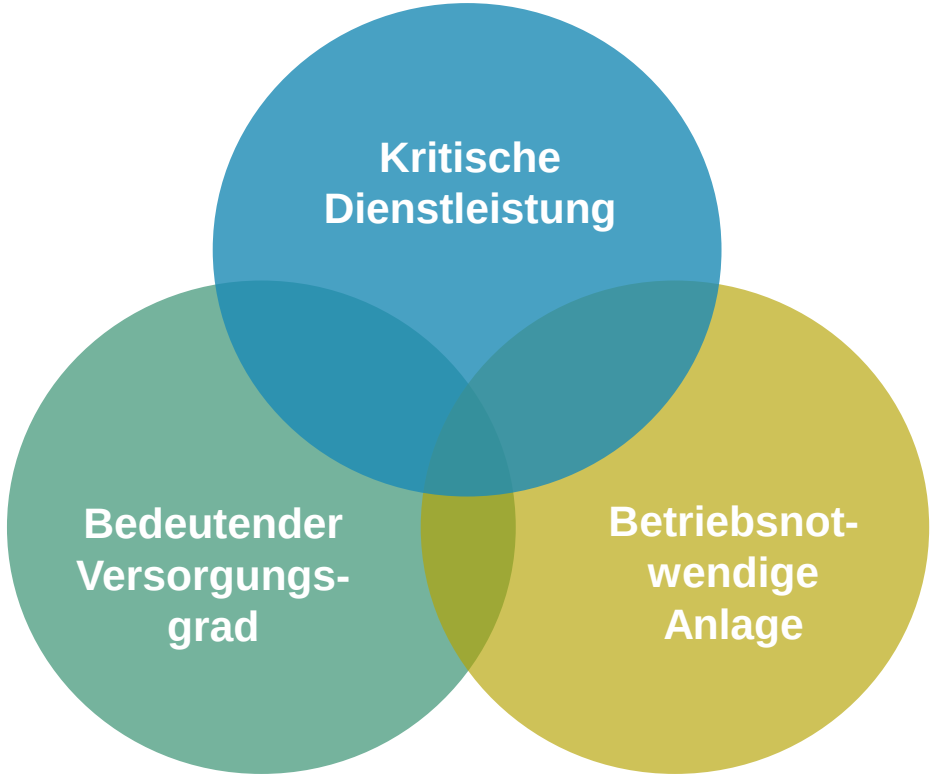
Kritische Komponente

- **Komponenten**,
  - die in Kritischen Infrastrukturen **eingesetzt** werden,
  - bei denen **Störungen** zu Ausfall / erheblicher Beeinträchtigung der Kritischer Infrastrukturen oder zu Gefährdungen für die öffentliche Sicherheit führen können und
  - die auf Grund eines **Gesetzes** als kritische Komponente **bestimmt** werden oder eine auf Grund eines Gesetzes als kritisch bestimmte Funktion realisieren.
- **Folgen**
  - Komponenten dürfen nur eingesetzt werden, wenn Hersteller Garantieerklärung abgegeben haben. Daraus muss hervorgehen, wie Komponenten gegen Sabotage geschützt werden.
  - Keine Rückwirkung

Bislang keine kritischen Komponenten im Energiesektor

Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (KritisV)

Energie	Wasser	Ernährung	IT / TK
Gesundheit	Finanzen u. Versicherung	Transport u. Verkehr	



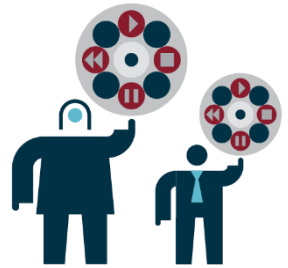
Bestimmt durch BSI-Kritisverordnung

#3 Wer ist Betreiber einer Kritischen Infrastruktur in der Energiebranche?

Schwellenwerte nach der neuen **KritisV** (seit 1. Januar 2022)

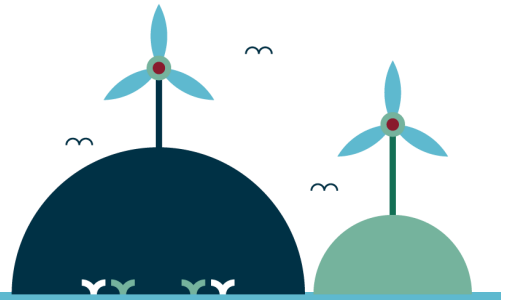
Anlagenkategorie	Bemessungskriterium	Schwellenwerte BSI-KritisV
Erzeugungsanlage	Installierte Nettonennleistung in MW	**104**
	Installierte Nettonennleistung in MW, wenn als Schwarzstartanlage nach BK6-18-249 kontrahiert	0
	Installierte Nettonennleistung in MW, wenn Anlage zur Erbringung von Primärregelleistung nach § 2 Nr. 8 StromNZV präqualifiziert ist	36
Anlage oder System zur Steuerung/Bündelung elektrischer Leistung	Installierte Nettonennleistung in MW	**104**
	Installierte Nettonennleistung in MW, wenn als Schwarzstartanlage nach BK6-18-249 kontrahiert	0
	Installierte Nettonennleistung in MW, wenn Anlage zur Erbringung von Primärregelleistung nach § 2 Nr. 8 StromNZV präqualifiziert ist	36
Zentrale Anlage/System für den Stromhandel	Handelsvolumen in TWh/Jahr	3,7
Übertragungsnetz	entnommene Jahresarbeit GWh/Jahr	3.700
Verteilnetz	entnommene Jahresarbeit GWh/Jahr	3.700

Wer ist Betreiber?



Betreiberbegriff gemäß KritisV	• „Eine natürliche oder juristische Person, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände **bestimmenden Einfluss** auf die Beschaffenheit und den Betrieb von Anlagen oder Teilen davon ausübt."
Verordnungs-begründung:	• Betreiber ist nach immissionsschutzrechtlichem Verständnis, wer – **weisungsfrei und selbständig** über Anlagen verfügt und – die tatsächliche Sachherrschaft über die Anlage besitzt, was meist mit der **rechtlichen Verfügungsgewalt** verknüpft ist, wer also – die Verfügungsgewalt **in eigener Verantwortung** ausübt.
Fazit	➢ Unbeachtlich, wenn sich Betreiber beim Betrieb der Anlage oder der erforderlichen IT-Systeme IT-Dienstleister bedient, sofern er bestimmenden Einfluss nicht aufgibt.

Betreiber Kritischer Infrastrukturen



Projektgesellschaft

- Anlagenkategorie: Erzeugungsanlage
- Windpark > 104 MW

➢ Projektgesellschaft ist Betreiber einer Kritischen Infrastruktur

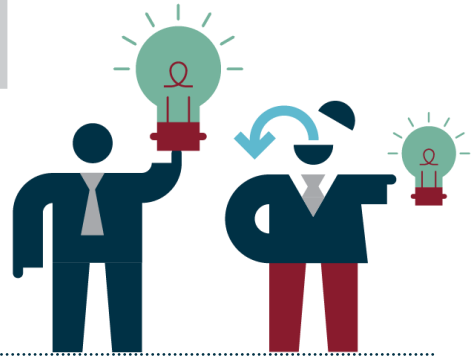
Betriebsführer

- Anlagenkategorie: Anlage oder System zur Steuerung/Bündelung elektrischer Leistung
- Portfolio > 104 MW

➢ Betriebsführer ist Betreiber einer Kritischen Infrastruktur

Einordnung des Umspannwerks in die KritisV

	Umspannwerk Bestandteil des öffentlichen Netzes	**Umspannwerk nicht Bestandteil des öffentlichen Netzes**
Kategorie	Übertragungsnetz/Verteilnetz	Anlage oder System zur Steuerung/Bündelung elektrischer Leistung
Schwellenwert	3.700 GWh/Jahr	104 MW
Betreiber	Netzbetreiber	BSI: Direktvermarkter ist Betreiber und Infrastrukturgesellschaft ist Dienstleister des Direktvermarkters



#4 Umsetzungspflichten und -fristen

Pflichten von Betreibern Kritischer Infrastrukturen

	BSIG (§ 8a Abs. 1)	EnWG (§ 11 Abs. 1a, 1b)
Adressat	Betreiber von (allgemeinen) **Kritischen Infrastrukturen,** z.B. Anlage oder System zur Steuerung/Bündelung elektrischer Leistung	Betreiber von **Energieanlagen** und **Netzbetreiber**
Compliance	Umsetzung **Stand der Technik** • i.d.R. ISMS nach ISO 27001 • Einzelnachweis mit BSI • Nachweis durch Umsetzung **b**ranchen**s**pezifischer **S**icherheits**s**tandards (**B3S**) • Ab dem 1. Mai 2023: Einsatz von Systemen zur Angriffserkennung ➡ Nachweis über Einhaltung **erstmals nach 2 Jahren** und danach **alle 2 Jahre** (gem. § 8a Abs. 3)	**IT-Sicherheitskataloge** der BNetzA • ISMS nach ISO 27001 • Zertifizierung bei akkreditierter Zertifizierungsstelle • Ab dem 1. Mai 2023: Einsatz von Systemen zur Angriffserkennung ➡ IT-Compliance bei Umsetzung und regelmäßige Überprüfung ➡ Umsetzungsfrist bereits abgelaufen
Registrieren & Kontaktstelle benennen	• Registrierung beim BSI und Benennen einer Kontaktstelle • Bis zum ersten Werktag, nach dem man Betreiber einer Kritischen Infrastruktur wurde ➢ Eine Anlage gilt ab dem **1. April** des Kalenderjahres, das auf das Kalenderjahr folgt, in dem ihr Versorgungsgrad den genannten Schwellenwert erstmals erreicht oder überschreitet, als Kritische Infrastruktur	
Meldepflichten	• ***Offen*** falls Störungen die Leistung beeinträchtigen und für Ausfälle gesorgt haben • ***Anonym*** bei erheblichen Störungen, die zu Beeinträchtigungen oder Ausfällen führen können	

Systeme zur Angriffserkennung (Intrusion Detection Systems (IDS)

- Aktive Überwachung von Computersystemen und/oder -netzen mit dem Ziel der Erkennung von Angriffen und Missbrauch
- In den meisten Fällen kann auf eine **manuelle Prüfung** der Auswirkungen des Angriffs aber nicht verzichtet werden
- Der Begriff "Angriffserkennungssysteme" bezieht sich auf eine große Bandbreite an Maßnahmen. Das BSI wird zur Definition eine Orientierungshilfe herausgeben
- Anschaffungs-, Wartungs- und Betriebskosten von IDS gleichermaßen wichtig. Der Betriebsaufwand hängt von der Nutzungsfreundlichkeit des IDS ab

Verpflichtender Einsatz ab dem 1. Mai 2023

#5 Ausblick: Cybersicherheitsagenda, NIS-Richtlinie 2 und Cyber Resilience Act

Cybersicherheitsagenda des BMI

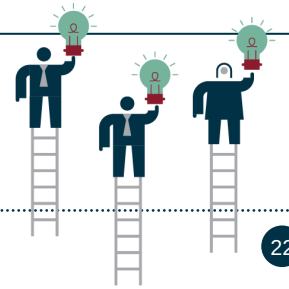
- Förderung von Investitionen für Cyber-Resilienzmaßnahmen in KMU, die dem KRITIS-Sektor angehören
- Berücksichtigung der Sicherheit von IT-Lieferketten im Rahmen der gesetzlichen KRITIS-Regulierung
- Einrichtung von Awareness- und Cyber-Resilienz-Projekten, die vom BSI und von externen Dienstleistern angeboten werden
- Für jeden KRITIS-Sektor soll ein sektorspezifisches Cyber Emergency Response Team (CERTs) von den KRITIS-Betreibern etabliert werden

Directive on Security of **N**etwork and **I**nformation **S**ystems 2 (NIS 2)

- Am **13. Mai 2022** haben sich der Rat, das Europäische Parlament und die Kommission im Rahmen der Trilogverhandlungen auf einen Entwurf für eine reformierte Richtlinie über Netze und Informationssysteme (NIS2) geeinigt
- Der Entwurf muss **noch** vom Rat und dem Europäischen Parlament **formal gebilligt werden**
- Nach Einigung und Inkrafttreten haben Mitgliedstaaten **21 Monate** Zeit, die Richtlinie umzusetzen

Neuerungen durch die NIS 2

Anwendungsbereich	Sektorunternehmen **ab 10 Mio. Jahresumsatz** oder mehr als **50 Mitarbeitern,** die Kritikalitätskriterien erfüllen. Unabhängig von Größe, wenn Dienst wesentlich für öffentliche Sicherheit oder Störung des Dienstes wesentliche Systemrisiken verursachen könnte.
Register für Sicherheitslücken	ENISA soll ein europäisches **Register für Sicherheitslücken** entwickeln und pflegen.
Risikomanagement	Cybersicherheitsmaßnahmen sollen nunmehr auch die **Personalsicherheit, Zugangskontrollpolitik und Anlagenverwaltung** umfassen.
Meldepflicht reduziert	Die Verpflichtung zur Meldung erheblicher Störungen, die zu Beeinträchtigungen oder Ausfällen **führen können**, wird gestrichen.
Bußgelder erhöht	Bußgeld von max. **4 Mio. Euro** oder 2 % des weltweiten Jahresumsatzes für Kritische Infrastrukturen.
Lieferkette	Direkte Lieferanten müssen über solide Cybersicherheitsmaßnahmen verfügen.



Vielen Dank für Ihre Aufmerksamkeit!

Dr. Karla Klasen
Senior Associate
Germany

+49 221 5108 4270
karla.klasen@osborneclarke.com

Dr. Karla Klasen berät Mandanten in energierechtlichen Fragestellungen. Sie ist auf Erneuerbare-Energien-Projekte, Elektromobilität und Rechtsfragen bezüglich der Digitalisierung der Energiewirtschaft spezialisiert.

Schwerpunktmäßig berät sie Investoren, Finanzierer, Asset Manager, Dienstleister und Energieversorgungsunternehmen zu regulatorischen und kommerziellen Fragen im Bereich der erneuerbaren Energien. Im Bereich der Elektromobilität berät sie Mandanten zu regulatorischen Aspekten der Ladeinfrastruktur und unterstützt sie bei der Vertragsgestaltung.