

Dealing with cyber threats

Recognize, react and secure

Speakers



Helmut Brechtken

Financial Advisory
Partner | Head of Digital Forensic Incident Response
Deloitte GmbH

Phone: +49 221 9732 4949
E-mail: hbrechtken@deloitte.de



Nikola A. F. Werry, LL.M. (UK)

Digital Law | Head of Data and Data Protection Law
Partner, Rechtsanwalt (German Attorney at Law)
Deloitte Legal Rechtsanwaltsgesellschaft mbH

Phone: +49 69 71918 8482
E-mail: nwerry@deloitte.de



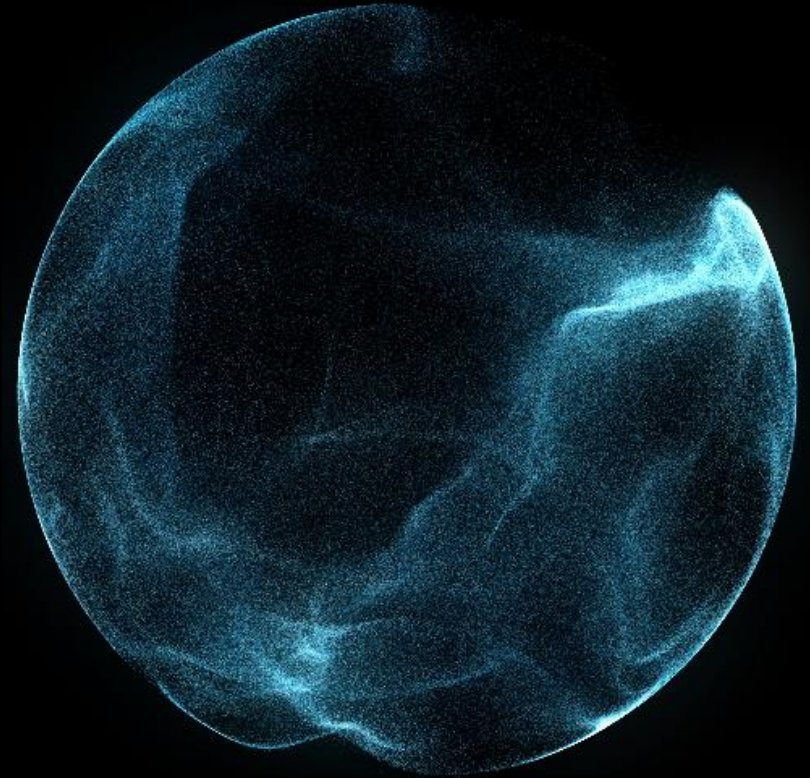
Frank Fischer, LL.M. (Univ. London)

Banking & Finance | Head of Insurance & Invest. Mgmt
Partner, Rechtsanwalt (German Attorney at Law)
Deloitte Legal Rechtsanwaltsgesellschaft mbH

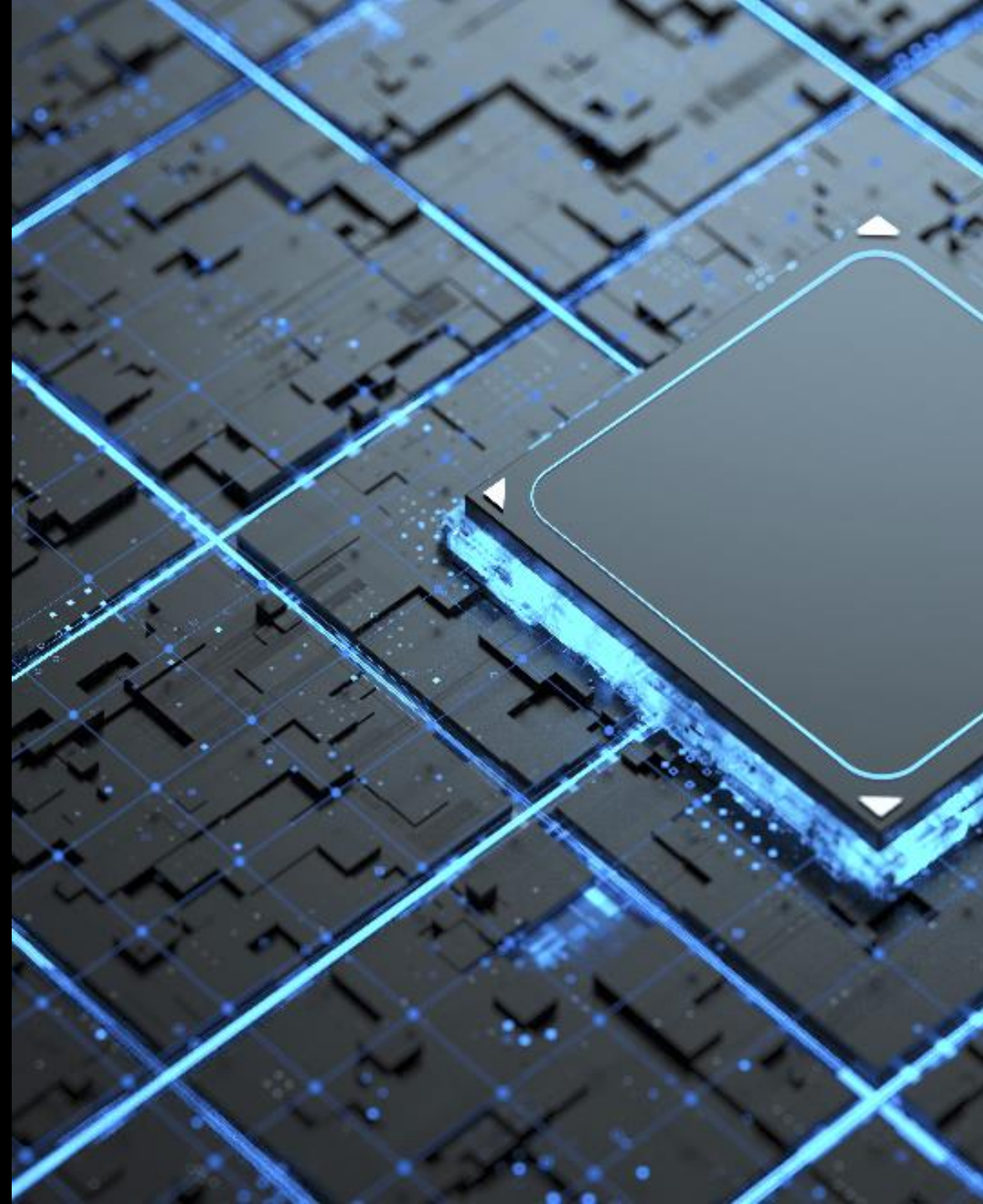
Phone: +49 89 29036 5680
E-mail: frankfischer@deloitte.de

AGENDA

1. Welcome / Introduction
2. Overview of typical / current attack scenarios
3. Responding to cyber attacks from a legal perspective
4. Insurance cover and settlement of claims
5. Q&A

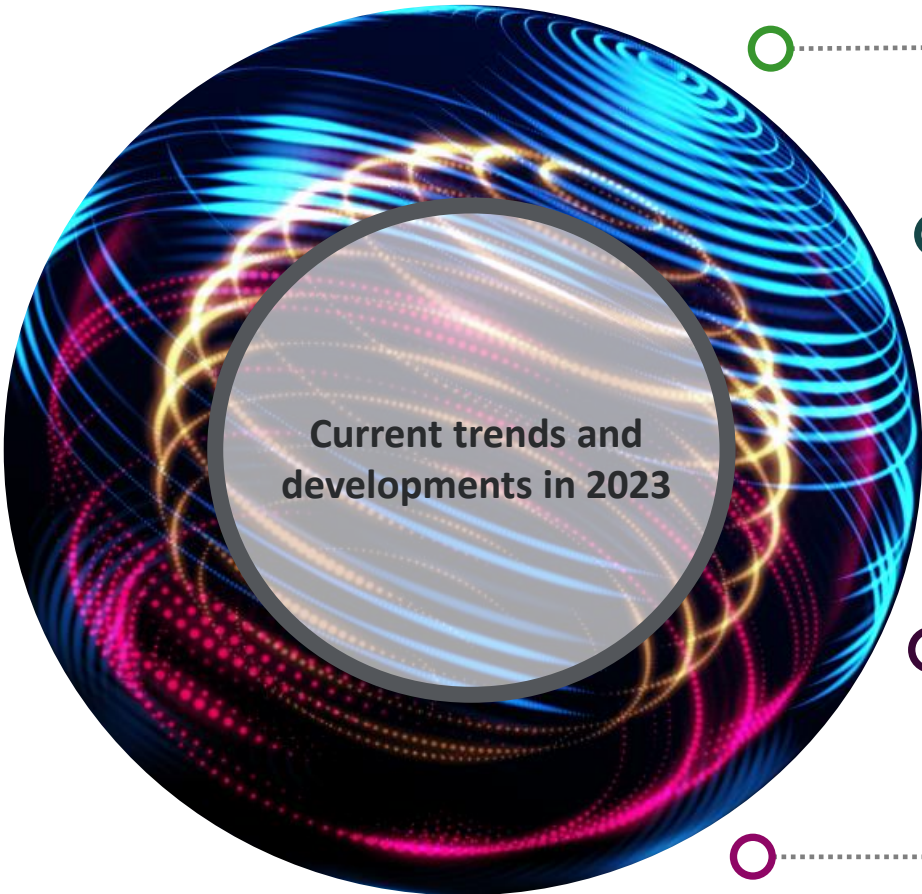


Overview of typical / current attack scenarios and their impact on companies



Cybercrime trends in 2024

Our perception



Current trends and developments in 2023



Payment Diversion Fraud (Bank data fraud)

Fraudsters spy on e-mail communications and inform you that your bank details have changed.

CEO Fraud (Fake President Fraud, "boss scam")

A fraudster pretends to be the boss and asks employees to take action (e.g. transfer money)

Ransomware (Encryption/extortion Trojans)

Attackers extort money by demanding a ransom to decrypt or not disclose data.

Advanced Persistent Threat (Complex malware)

Attackers carry out sophisticated, targeted attacks (e.g. to steal data and access data).

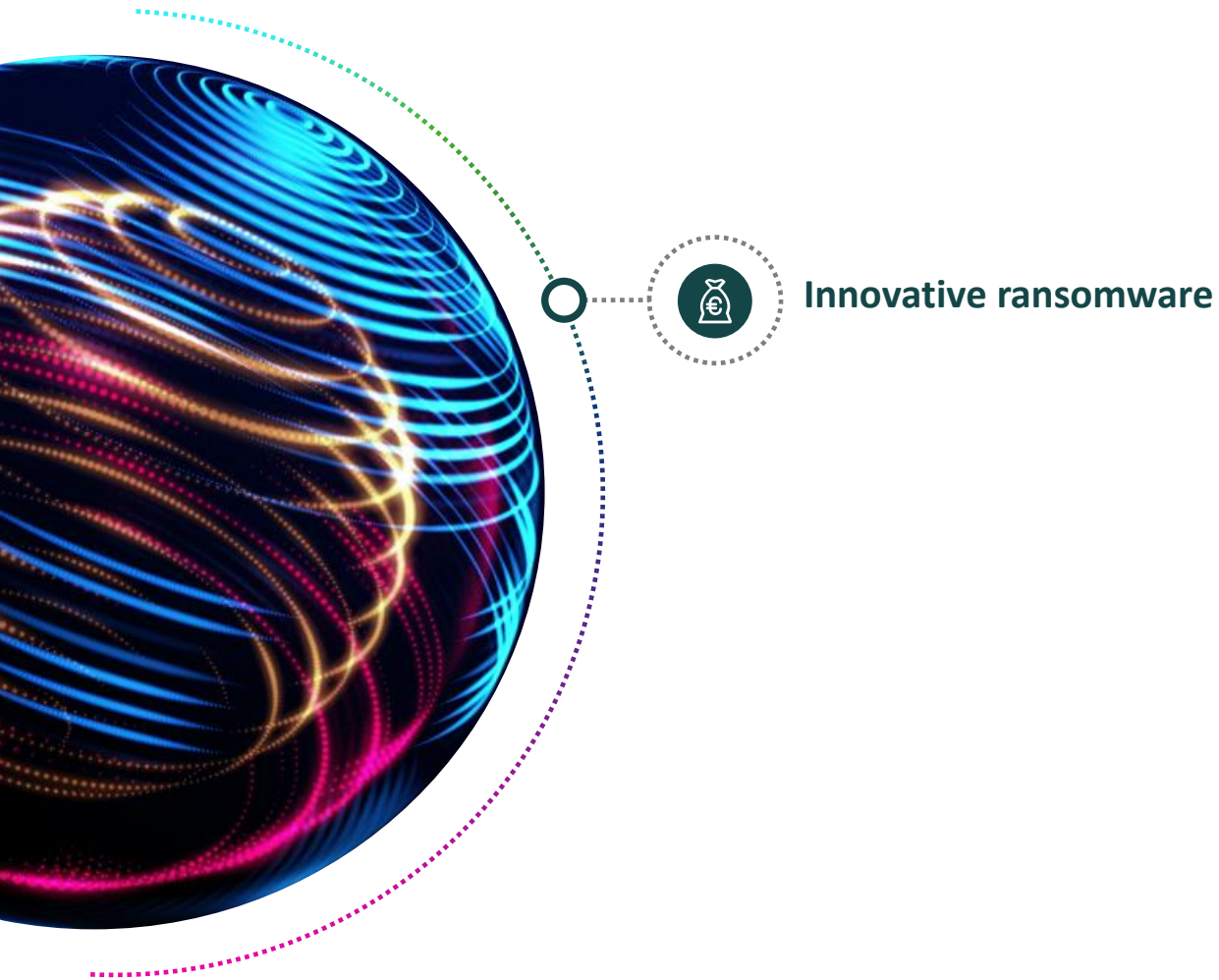
Insider Fraud (Threat from within)

A fraudster with authorized access in an organization misuses it to negatively influence important information or systems.

Trend	Costs
	€€€
	€€€
	€€ - €€€
	€€€
	€ - €€€

Current trends

Exposure to cybercrime in Germany





The evolution of cyber extortion

The evolution of cyber extortion since around 2018

Traditional (V1)	Blackmail through data encryption
V2	+ Destruction of the backups
V3	+ Data extraction
V4	Data leakage WITHOUT encryption, blackmail by threatening to publish data
V5 - current	Data leakage WITHOUT encryption, extortion of the target AND the data owner with data publication
V6 - ???	

Please note:

 Criminal charges if applicable

 Risk of criminal offense / possible penalties for ransom payment

Responding to cyber attacks from a legal perspective



Handling and processing cyber incidents from a legal perspective

Response. Recover. Thrive.

1



Response

- Identification / initial documentation
- Damage limitation
- Securing evidence
- Reporting obligations / rights of data subjects
- Replacement procurement
- Communication

2



Recover

- Detailed legal assessment of the incident
- Compliance recovery
- (Further) damage limitation

3

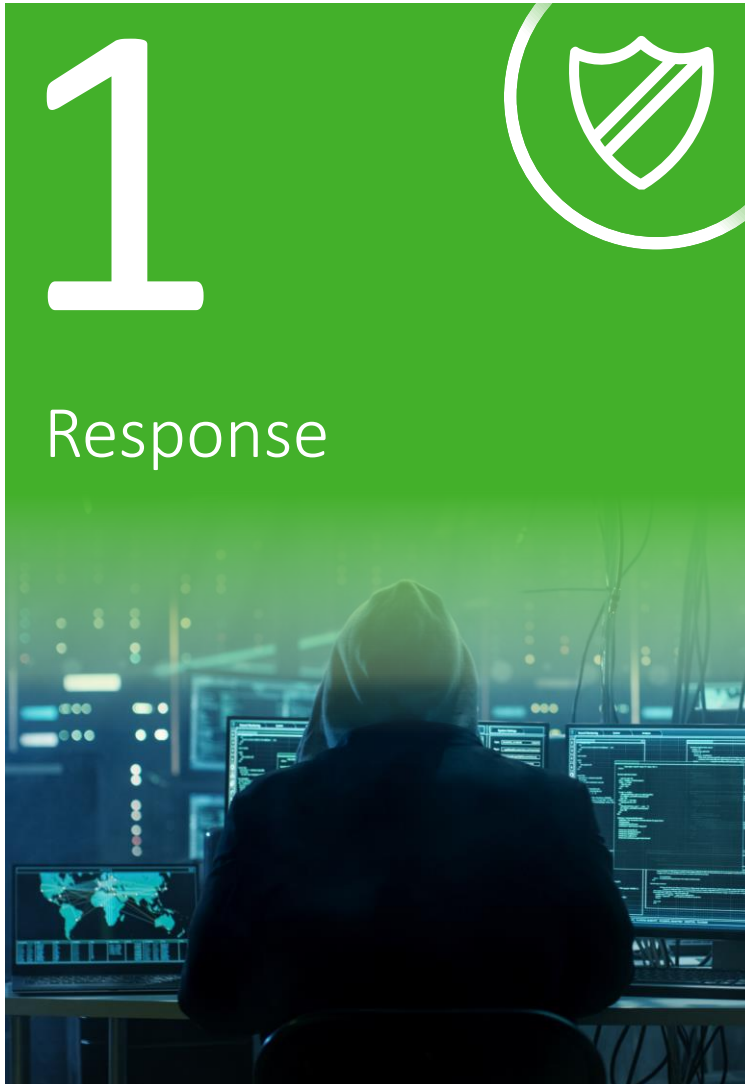


Thrive

- Implementation of the findings
- Training and sensitization
- Cooperation with the authorities
- Insurance claims

Handling and processing cyber incidents from a legal perspective

Response



Identification and initial documentation

- Early identification of the incident
- Documentation of the incident (facts and measures)



Damage limitation

- Take immediate measures to prevent and limit damage



Securing evidence

- Ongoing legal assessment and preservation of evidence to avoid adverse legal consequences



Reporting obligations and data subject rights

- Taking the immediate measures required by law (e.g. reporting the incident)
- Fulfillment of requests from affected parties



Replacement procurement

- Carefully select short-term replacements

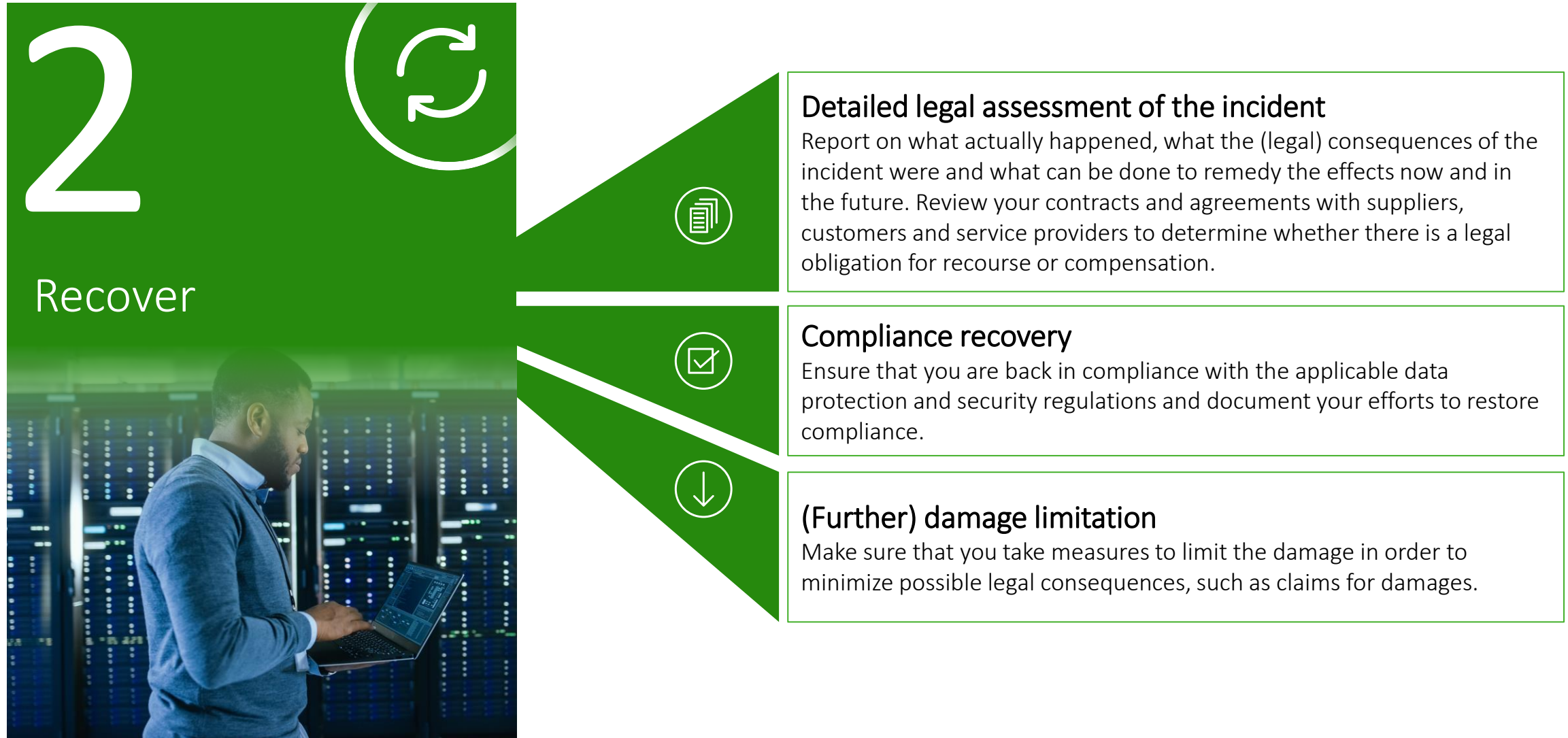


Communication

- Communication with stakeholders to avoid risks

Handling and processing cyber incidents from a legal perspective

Recover



Handling and processing cyber incidents from a legal perspective

Thrive



Implementation of the findings

The results of the previous phase (in particular the in-depth analysis of the incident and the identified improvements to the compliance organization) are implemented.

Training and sensitization

Introduction of training and education programs to raise awareness of cyber security. Focus: Compliance with and understanding of regulatory requirements.

Cooperation with authorities

Continued cooperation with the competent criminal investigation / data protection authorities.

Insurance claims

Disputes with insurance companies, especially if the claim is (partially) disputed. This may be the case in particular if duties of care were allegedly not complied with.

Insurance cover and settlement of claims



Insurance cover and settlement of claims

Effective cyber protection requires a structured and long-term approach

1



In the run-up to the insurance contract

- Analysis of risks and needs
- Things to note before/when concluding the contract

2



During the contract term

- Continuous monitoring
- Contractual obligations

3



In the event of a specific claim

- Reporting and notification obligations
- Adjustment of risk management

Insurance cover and settlement of claims

In the run-up to the insurance contract



Risk analysis

- Identification of the vulnerable IT infrastructure
- Analysis of the specific business environment, possible threat scenarios, etc., including taking into account regulatory requirements, e.g. FS, KRITIS



Determination of requirements (sum insured)

- Needs-based determination of the relevant sums insured
- Third-party/own damage: Essential components (operational failure, restart, etc.)



Insurance cover within the group

- Ensuring that all affected companies in the group are covered
- Dynamic integration of future group companies as well



Coordination with the insurer

- Clear designation of the scope of cover
- Clear communication channels and responsibilities, including in the event of a claim



Duty of disclosure

- Compliance with pre-contractual obligations vis-à-vis the insurer
- Truthful answers to questionnaires on IT security and system standards

Insurance cover and settlement of claims

During the contract term



Ongoing risk analysis

- Identification of new risks or changes to the scope of risk



Updating the sum(s) insured

- Adjustment to increase or change in risks



Compliance with any obligations

- Implementation of regular software updates, "state of the art"



Insurance cover within the Group

- Regular consideration of (new) companies and (new) business models



Internal structures and measures

- Documentation and training, emergency/response plans, damage management

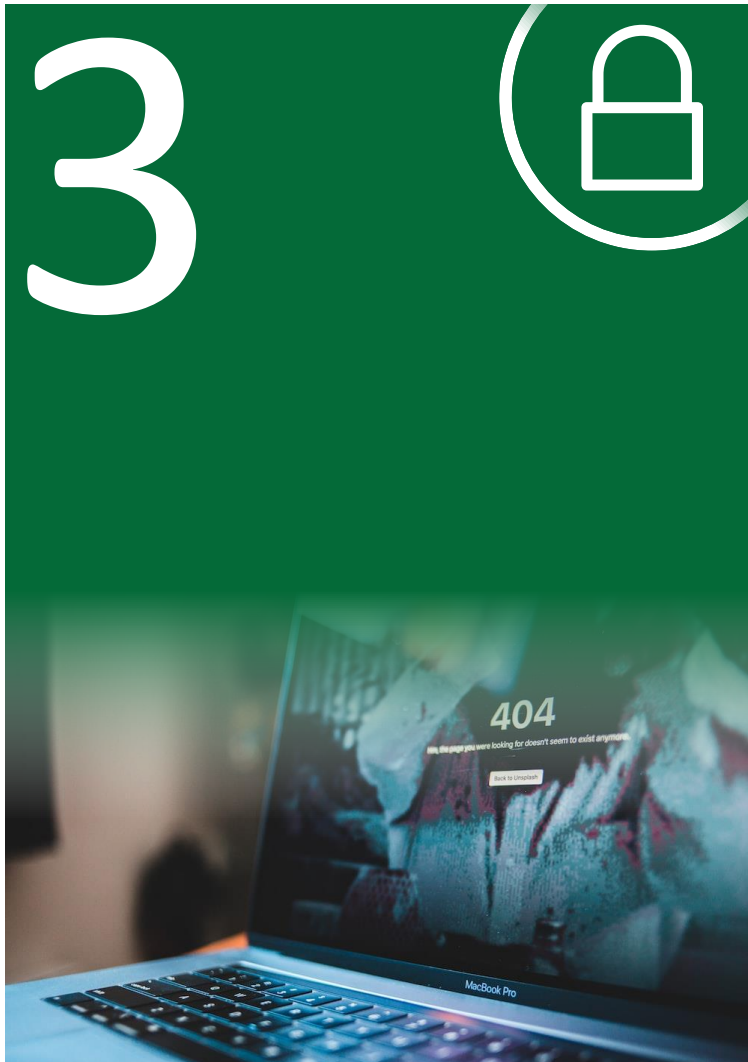


Insurance contract management

- Overview and timely action regarding renewal, termination, etc.

Insurance cover and settlement of claims

In the event of a specific claim



Damage report

- Immediate notification of the claim to the insurer



Minimizing the damage

- Obligation to minimize damage, if necessary with external consultant support
- Limitation of data protection incidents, technical containment, etc.



Cooperation with external service providers

- Exchange with forensics, for example, to restore IT as quickly as possible
- Cooperation with experts to determine possible (personal) damage



Restoring the ability to work

- Quick restart of essential IT, use of internal plans/communication



Communication with authorities/damaged parties

- Continuous discussions with (data protection) authorities or injured parties (liability) lead to minimization of damage and, if necessary, faster claims settlement by insurers



Internal structures and measures

- Optimization of IT/elimination of security gaps to prevent future attacks
- Adaptation of relevant processes/documentation, lessons learned from the loss event

Q&A



Many thanks for
your participation





Further information

Your contact Helmut Brechtken



Helmut Brechtken

Partner
Head of Digital Forensic Incident Response

Graduate physicist
Certified ISO/IEC 27001 Lead Auditor

Helmut Brechtken is a partner in the Forensic Service Line at Deloitte and has more than 25 years of professional experience in consulting and the chemical industry.

He has led over 300 digital forensics and cyber incident response investigations and projects. He has extensive experience in conducting complex eDiscovery proceedings from national and international investigations, such as investigations by the US Department of Justice (DoJ) and the US Securities and Exchange Commission (SEC).

Your contact Frank Fischer



Frank Fischer, LL.M. (Univ. London)

Partner

Banking & Finance | FSI | Head of Insurance & Investment Management

Rechtsanwalt (German Attorney at Law)

Frank Fischer has been working as a lawyer in the Legal Financial Services sector for more than 15 years and is the partner in charge of Deloitte Legal's insurance and investment management divisions in Germany.

He advises primary insurers and reinsurers, insurance intermediaries, IORPs, banks, financial service providers and asset managers in all areas of regulatory law and the interfaces with corporate law and other areas. He regularly assists his clients in transactions, in transformation projects and in proceedings before BaFin.

Before joining Deloitte Legal, Frank was a lawyer at another Big4 law firm and Assistant General Counsel of a leading asset manager for institutional investors. He has extensive experience in solving cross-jurisdictional problems in corporate groups as well as advising managers on liability, structural and organizational issues (corporate governance & compliance).

Your contact Nikola Werry



Nikola A. F. Werry, LL.M. (UK)

Partner

Digital Law | Head of Data & Data Protection Law

Rechtsanwalt (German Attorney at Law)

Nikola Werry is a partner at Deloitte Legal in Frankfurt am Main and works in the Digital Law service line. Nikola's professional focus is on data and data protection law and legal issues relating to digitalization. She has broad experience in supporting and advising national and international companies on aspects related to the legally compliant conceptualization and implementation of digital products, strategies and business models. Through her experience in the market and her expertise in leading multidisciplinary teams in the context of complex consulting projects, Niko not only supports her clients with the legal challenges of a project, but also advises them on how to overcome the numerous organizational, economic and procedural challenges they face in the course of a project.

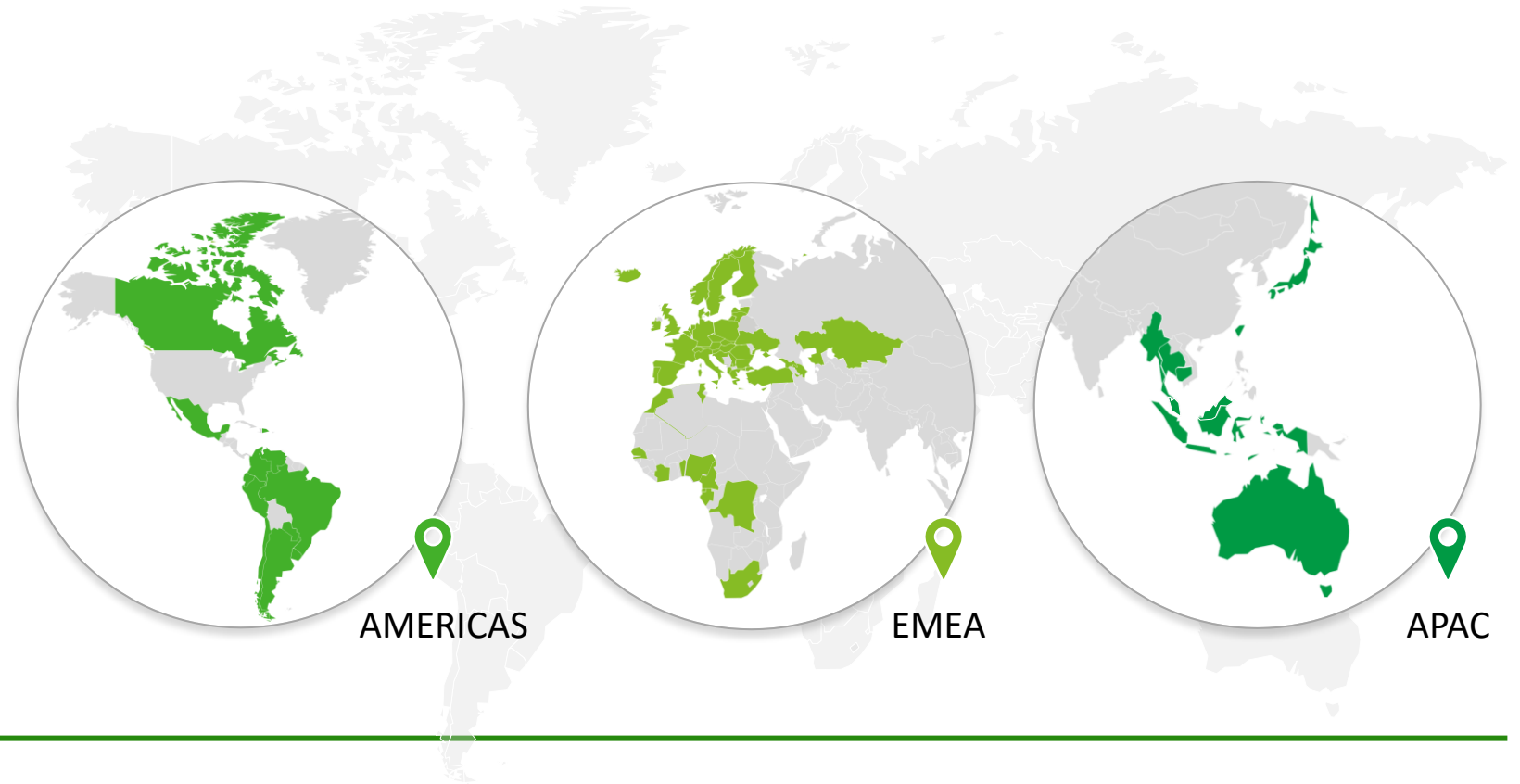
Niko regularly gives lectures, workshops and webinars on various topics in the field of digitalization and regularly publishes specialist articles. She is also the editor and author of the handbook "Datenrecht in der Digitalisierung" (Data Law in Digitalization), which illuminates and defines data law in its individual facets for the first time. Niko is also the founder of a specialist network for data law and digitization and a board member of the Research Center for Legal Issues of New Technologies and Data Law (ForTech) at the University of Bonn.

It is listed among the "Ones to Watch 2024" in the Best Lawyers Ranking in the area of Data Security and Privacy Law.

Deloitte Legal has a strong global presence

It can be very challenging to coordinate a large number of legal advisors around the world without losing sight of individual aspects.

As one of the world's leading legal consultancies, Deloitte Legal helps you overcome challenges and realize your vision by being your single point of contact for your global legal needs.



Deloitte Legal practices

AMERICAS

1. Argentina
2. Brazil
3. Canada
4. Chile
5. Colombia
6. Costa Rica
7. Dominican Republic
8. Ecuador
9. El Salvador
10. Guatemala
11. Honduras
12. Mexico
13. Nicaragua
14. Paraguay
15. Peru
16. Uruguay
17. Venezuela

EMEA

1. Albania
2. Austria
3. Azerbaijan
4. Belgium
5. Benin
6. Bosnia and Herzegovina
7. Bulgaria
8. Cameroon
9. Croatia
10. Cyprus
11. Czech Republic
12. Dem. Rep. of Congo
13. Denmark
14. Equatorial Guinea
15. Finland
16. France
17. Gabon
18. Georgia
19. Germany
20. Greece
21. Hungary
22. Iceland
23. Ireland
24. Italy
25. Ivory Coast
26. Kazakhstan

27. Kosovo
28. Latvia
29. Lithuania
30. Malta
31. Morocco
32. Nigeria
33. Norway
34. Poland
35. Portugal
36. Romania
37. Senegal
38. Serbia
39. Slovakia

APAC

40. Slovenia
41. South Africa
42. Spain
43. Sweden
44. Switzerland
45. The Netherlands
46. Tunisia
47. Turkey
48. Ukraine
49. United Kingdom
1. Australia
2. Cambodia
3. Hong Kong SAR, China
4. Indonesia
5. Japan
6. Malaysia
7. Myanmar
8. Singapore
9. Taiwan
10. Thailand

Experience the future of legal advice now

Deloitte Legal, these are

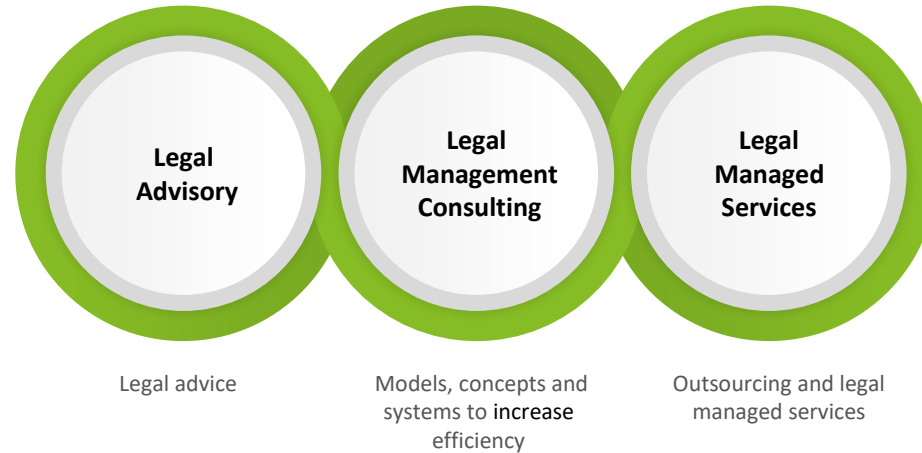
more than **2.500** Lawyers
in **75+** Countries



who work closely together
across national borders and together with
other Deloitte business units

Services from Deloitte Legal

Our three overlapping service areas enable us to advise our clients when and where needed and in the most suitable form to realize their visions.



We create (added) value

As part of Deloitte's global network, Deloitte Legal works with a wide range of other disciplines to provide multinational legal solutions and integrated services worldwide:



in harmony
with your company-wide vision



customized
for your business units and branches



technology-based
for improved cooperation and transparency



coordinated
to your regulatory requirements



Deloitte Legal refers to the legal practices of Deloitte Touche Tohmatsu Limited member firms, their affiliates or partner firms that provide legal services.

This publication contains only general information which is not intended to address the specific circumstances of any particular case and is not intended to form the basis of any commercial or other decision. Neither Deloitte Legal Rechtsanwaltsgesellschaft mbH nor Deloitte Touche Tohmatsu Limited, its member firms or their affiliates (collectively, the "Deloitte Network") are providing professional advice or services by means of this publication. None of the member firms of the Deloitte network is responsible for any loss of any kind suffered by any person in reliance on this publication.

Deloitte refers to Deloitte Touche Tohmatsu Limited ("DTTL"), a private company limited by guarantee, its network of member firms and its affiliates. DTTL and each of its member companies are legally autonomous and independent. DTTL (also known as "Deloitte Global") does not itself provide any services to clients. A more detailed description of DTTL and its member firms can be found at www.deloitte.com/de/UeberUns.

Deloitte provides audit, risk advisory, tax advisory, financial advisory and consulting services to companies and institutions from all sectors of the economy; legal advice is provided in Germany by Deloitte Legal. With a global network of member firms in more than 150 countries, Deloitte combines outstanding expertise with first-class services and supports clients in solving their complex business challenges. Making an impact that matters - for Deloitte's approximately 457,000 employees, this is both a shared mission statement and an individual aspiration.