Deloitte.
Legal



Protection of Government Classified Information in Industry

Opportunities & Challenges

Deloitte Legal Webcast November 18, 2026

Our Speakers



Dr. Söntje Julia Hilberg

Partner | Co-Lead, Digital Law
Deloitte Legal
Phone: +49 30 254683300
Email: shilberg@deloitte.de



Dennis Buschmann

Senior Manager | Attorney at Law
Deloitte Legal
Phone: +49 30 254681886
Email: dbuschmann@deloitte.de



Markus Göttemann

Senior Manager
Deloitte Cyber Strategy & Transformation
Phone: +49 30 254683623
Email: mgoettemann@deloitte.de

Agenda



01

Introduction to and Importance of the Protection of Classified Information

Transformation of the security market,
new ecosystems & supply chains

02

The Protection of Classified Information from a Legal Perspective

Legal Frameworks, Classified Information, Security Clearance Levels
as well as the dimensions of security classification

03

Operational Aspects of Physical and IT related Security Measures

Operational Implementation & Use Cases

01 Introduction to and Importance of the Protection of Classified Information

Market Transformation Due to the Changing Security Landscape

Increase: Security needs, cooperation, & network

New Actors

Start-ups and commercial technology providers are becoming integral parts of security-critical supply chains.

New supply chains

Collaboration is becoming broader, more international, and increasingly driven by software and data.

New Responsibilities

Security obligations extend to development, the cloud, maintenance, and subcontractors.



Challenge

- The deteriorating security environment is increasing both the volume of classified information and the level of protection required.
- At the same time, supply chains are becoming more complex and business processes are accelerating.

Perspective

- Protection of Classified Information is becoming the common protective framework that connects the various stakeholders across security-critical ecosystems and supply chains.
- Not only new market entrants must adapt their security and operating models; established industry players must also align with the evolving market environment and security landscape.

Protection of Classified Information as the Foundation for Collaboration in the Security Ecosystem

Market Positioning

- Established companies
- Companies with new business areas
- new companies

Stakeholders

- Industry / Small and Medium-Sized Enterprises
- Start-ups / Scale-ups
- Public Sector / Government

Roles

- Clients, Subcontractors
- Investors, IT providers, service providers, Consultants



Protection of Classified Information is the unifying protective element

It translates government security requirements into rules for people, organizations, facilities, IT, and contracts.

Personnel

Security clearance, need-to-know, roles

Physical

Access, storage, transport, Classified Information IT

Organizational

Security Management, Processes, Documentation, Incident Management

Contractual

Classified Information clauses, flow-down, Authority to Issue Instructions & Conduct Audits

02 The Protection of Classified Information from a Legal Perspective

Legal Framework for the Protection of Classified Information



SÜG

Act on Federal Security Clearance Procedures and the Protection of Classified Information



VSA

Classified Information Security Regulation (Verschlusssachenanweisung - VSA)



GHB

Industrial Security Manual (Geheimschutzhandbuch – GHB)

Protection of Classified Information & Classified Information



Protection of Classified Information

Classified Information

- Created through a formal classification by a competent authority
- The applicable classification level is determined by law



Trade secret

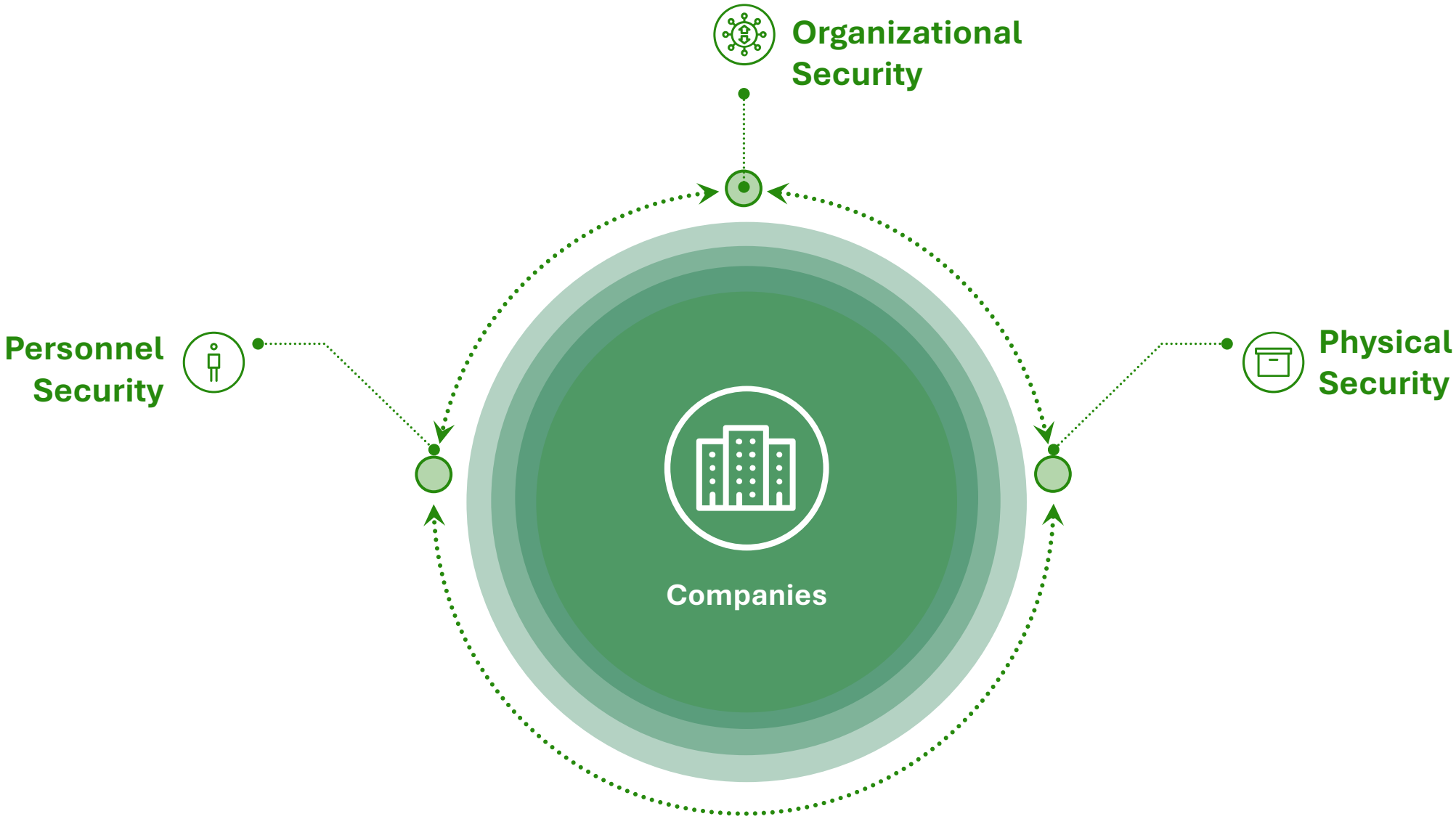


Contractual Confidentiality

Classification levels of classified information

For Official Use Only	Confidential	Secret	Top Secret
where unauthorized disclosure could be **detrimental** to the interests of the Federal Republic of Germany or one of its federal states (VS-Nur für den Dienstgebrauch – **VS-NfD**)	where unauthorized disclosure could be **harmful** to the interests of the Federal Republic of Germany or one of its federal states. (VS-Vertraulich – **VS-V**)	here unauthorized disclosure could endanger national security or cause serious harm to the interests of the Federal Republic of Germany or one of its federal states. (Geheim)	where unauthorized disclosure could endanger the existence or vital interests of the Federal Republic of Germany or one of its federal states (Streng Geheim)

Dimensions of the Protection of Classified Information within a Company



Dimensions of the Protection of Classified Information within a Company

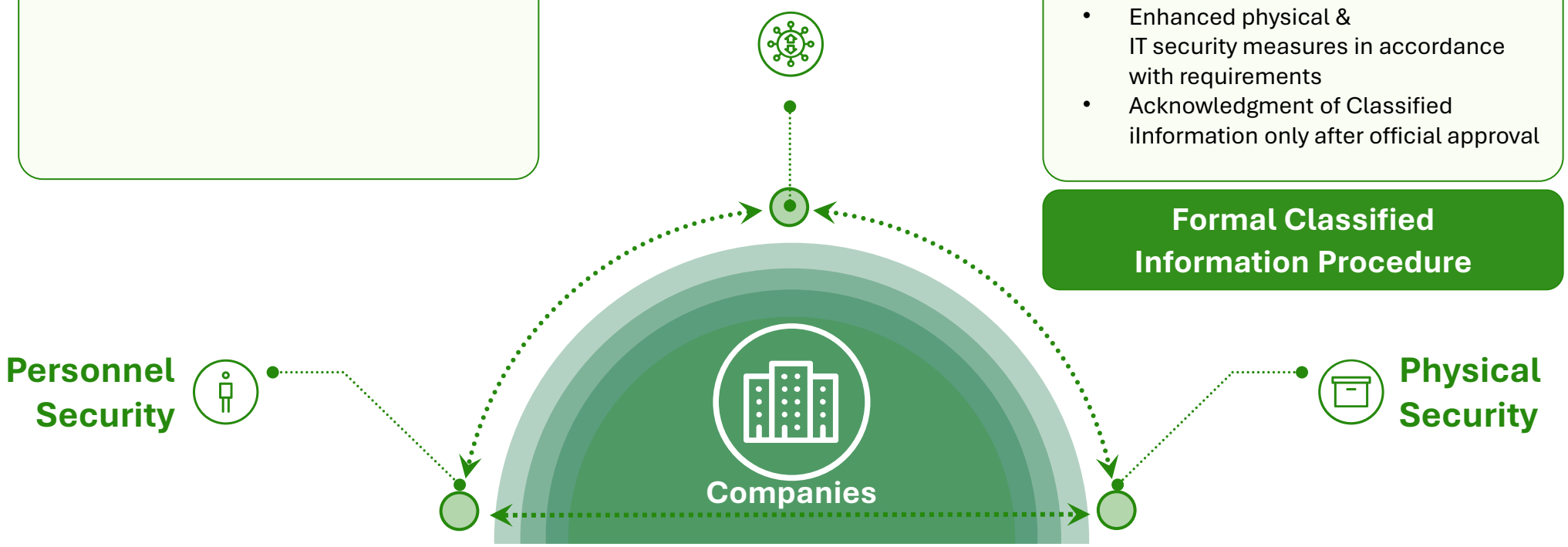
For Official Use Only

- No formal Classified Information Procedure needed; implementation of the GHB
- Employee authorization through internal commitment
- Appropriate physical & IT security measures

CONFIDENTIAL (+)

- Formalized Classified Information Procedure by the German government, inclduing the appointment of a Industrial Security Officer (Sicherheitsbevollmächtiger - SiBe)
- Security Clearance for employees according to the required level
- Enhanced physical & IT security measures in accordance with requirements
- Acknowledgment of Classified iInformation only after official approval

Formal Classified Information Procedure



Protection of Classified Information Extends Across the Entire Organization

Data Protection & Labor Law

Control vs. Transparency, Purpose Limitation & Employee Participation

Practice: Conducting a Security Clearance, access logs of employees

Contracts & Supply Chain

Security Requirements, Reporting Obligations & Flow-down

Practice: Workarounds for subcontractors not beeing ready to work with classifed information

Corporate & Governance

Accountability, Escalation, & Organizational Separation

Practice: Cross-departmental / cross-portfolio projects

Compliance & Regulation

Need-to-know vs. Investigation & Disclosure

Practice: Whistleblowing concerns project with classified information, anti-corruption, implementation of anti-money laundering measures

IT Security & Operations

Authorized Systems, Roles & Incident Response

Practice: Use of external services such as remote maintenance

Foreign Trade & International

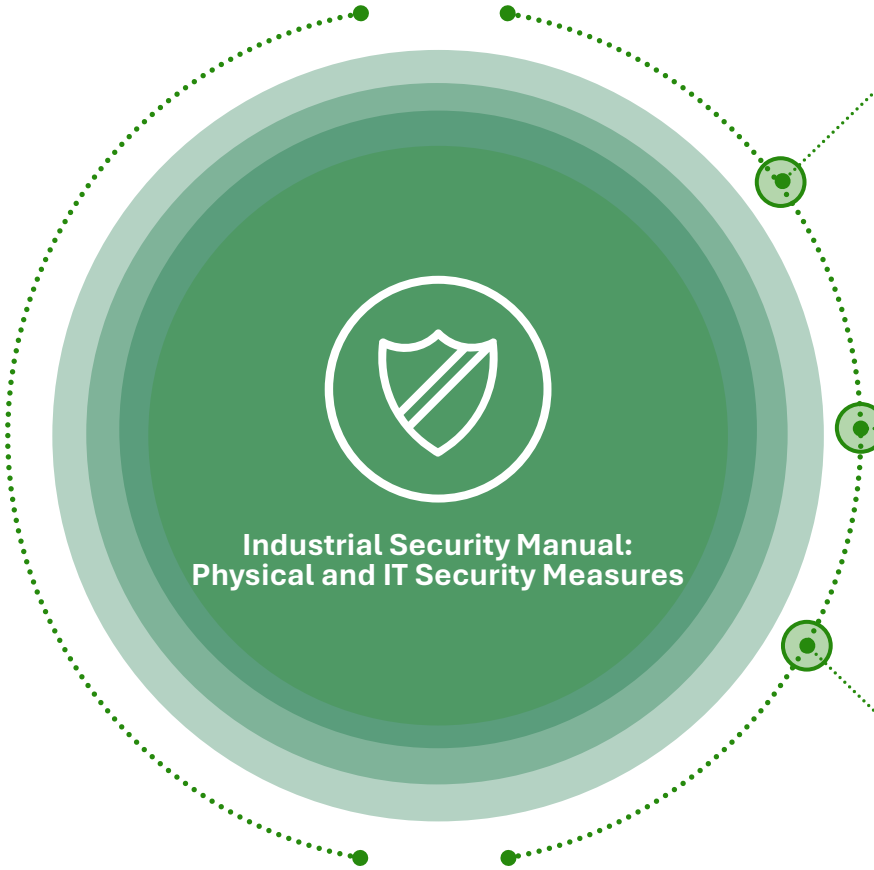
Export Controls & Cross-Border Flow of Sensitive Information

Practice: Cross-border collaboration (internal & external)

Objective: Identify areas of tension and synergy and develop risk-based solutions within a holistic strategic framework.

03 Operational Aspects of Physical and IT related Security Measures

From Regulations to Operational Implementation



Classified Information in Workflows

- Creation of Classified Materials
- Labeling
- Reproduction
- Need-to-know
- Record-Keeping
- Change in Classification Level
- Return & Destruction

Premises & Storage

- Restricted Areas
- Storage capabilities
- Surveillance
- Keys & Combination Locks
- Measures against peeping and eavesdropping

Classified IT & Incident Management

- Classified Information Processing & Storage
- Secure Communication
- Approved Systems
- Emergency and defense situations

Secure IT alone is not sufficient for classified information protection.

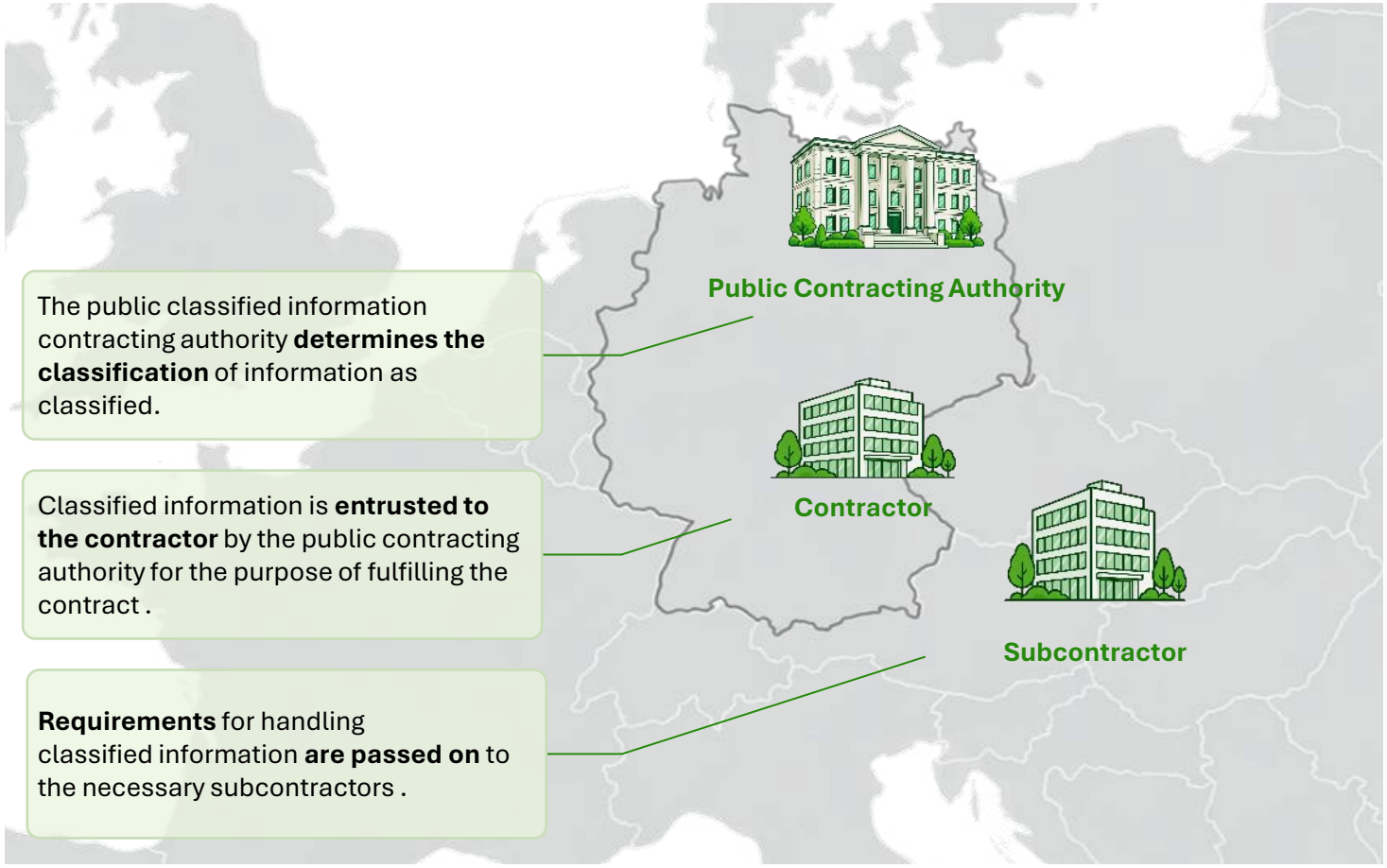
The specific use case determines the required scope of protection

Which parties are involved?

What information?

What environment?

Which processes?



The public classified information contracting authority **determines the classification** of information as classified.

Classified information is **entrusted to the contractor** by the public contracting authority for the purpose of fulfilling the contract .

Requirements for handling classified information **are passed on** to the necessary subcontractors .

Only once the use case is clear can a suitable and cost-effective classified IT infrastructure be designed.

The operational journey begins before the first classified item

Corporate Functions	Example Scenarios	Consequences
Sales	The client announces classified documents for the **preparation of a bid** .	Clarify requirements & prerequisites before receiving the materials.
Purchasing	A **supplier** needs some of the classified information for its **component**.	Clarify the permissibility of sharing and protection with the supplier.
Human Resources	**Several employees** are to work with the documents and need access.	Define access rights according to need-to-know-principle and train employees.
IT	The project team would like to **edit** and **save** the **documents digitally** .	Provide appropriate secure IT infrastructure and ensure IAM.
Facilities Management	The project team needs **premises** to work on the materials and hold meetings.	Organize access, secure storage, and visitor policies.

Classified information protection must be effective throughout the entire lifecycle and across all business units involved.

This is a hypothetical example and is not exhaustive.

VS-NfD Architectures: 3 Scenarios & Examples

Stand-alone client

Local Processing



- Dedicated VS-NfD client without network or Internet connection
- Approved hard drive encryption
- Data exchange via approved removable storage media

Local VS-NfD Network

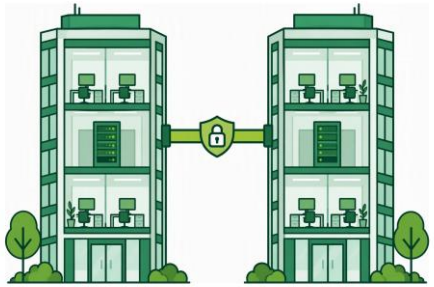
On-site Collaboration



- Local VS-NfD network with central services, e.g., email and file servers
- Additional operational and security functions, e.g., monitoring and PKI
- Use of BSI approved products, e.g., firewall, VPN service

Distributed VS-NfD Use

a) Site coupling



- Many regular users at another site
- Additional local VS-NfD network with approved site interconnection
- Dedicated operational processes for all VS-NfD networks

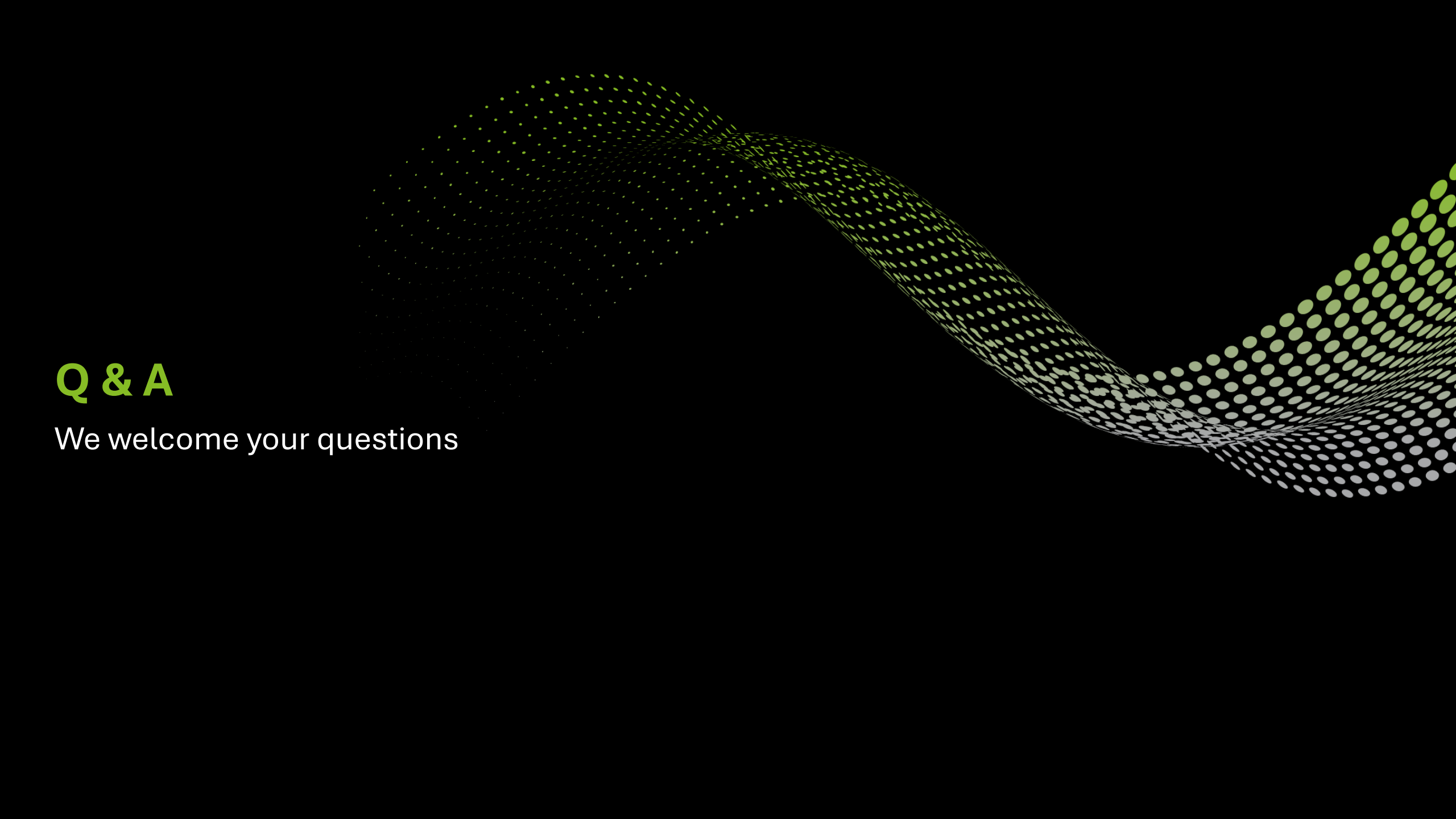
b) Remote Access



- Few or distributed users
- Dedicated VS-NfD client with an approved VPN service
- Access only after a connection is established; no additional VS-NfD network is required

VS-NfD capability requires a securely designed overall system, controlled network interfaces, and approved products for the respective security functions. Other confidentiality requirements remain unaffected.

Schematic AI illustrations. Authorizations apply to the respective intended use.


Q & A
We welcome your questions

Thank you very much

for your attention

Your contact



Dr. Söntje Julia Hilberg

Partner | Co-Lead Digital Law
Deloitte Legal
Phone: +49 30 254683300
Email: shilberg@deloitte.de



Dennis Buschmann

Senior Manager | Attorney at Law
Deloitte Legal
Phone: +49 30 254681886
Email: dbuschmann@deloitte.de



Markus Göttemann

Senior Manager
Deloitte Cyber Strategy & Transformation
Phone: +49 30 254683623
Email: mgoettemann@deloitte.de

Deloitte Legal has a strong global presence

Global presence combined with business expertise

We combine the scale and consistency of Deloitte Legal...

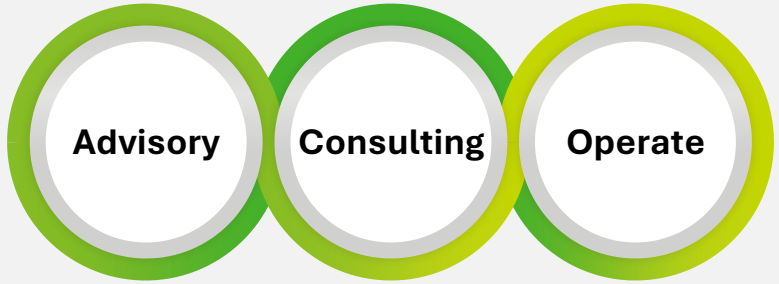
Deloitte Legal's practice areas are united by a shared DNA and a compelling track record of successful project implementations.



Seamless collaboration
across borders and with other Deloitte practices

... with a different legal perspective

While traditional legal advice reacts to individual events, Deloitte Legal helps companies create sustainable value—with integrated solutions for legal and business challenges.



Legal advice, strategy, processes, and technology for legal departments, as well as outsourced legal managed services.

As part of Deloitte, we combine **broad-based**, **internationally networked**, **cross-functional** and **technology-enabled** legal advice with **industry expertise** and a clear focus on practical, business-oriented solutions.

Deloitte Touche Tohmatsu Limited (DTTL) is the world's largest private professional services network and generated revenue of $70.5 billion in fiscal year 2025. With more than 470,000 employees worldwide, DTTL member firms provide services in the areas of audit, risk and financial advisory, tax, legal, and management consulting through offices in 150 countries and territories.

Deloitte.
Legal

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

Deloitte refers to Deloitte Touche Tohmatsu Limited (DTTL), its global network of member firms, and their affiliates (collectively, the "Deloitte Organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms, as well as their affiliates, are legally separate and independent entities that cannot bind or commit one another to third parties. DTTL, each DTTL member firm, and their affiliates are liable only for their own acts and omissions and not for those of the others. DTTL itself does not provide services to clients. For more information, visit www.deloitte.com/de/UeberUns.

Deloitte provides leading audit and advisory services to nearly 90% of the Fortune Global 500® companies and thousands of private companies. Legal services in Germany are provided by Deloitte Legal. Our people deliver measurable, long-term results that help strengthen public confidence in capital markets and support our clients through change and growth. Deloitte builds on 180 years of history and operates in more than 150 countries. Learn more about how Deloitte's approximately 460,000 employees live out the mission statement "making an impact that matters" every day: www.deloitte.com/de.

This publication contains only general information, and neither Deloitte Legal Rechtsanwaltsgesellschaft mbH nor Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, nor their affiliates (collectively, the "Deloitte Organization") are providing a professional service through this publication. This publication is not intended to serve as a basis for making business or financial decisions or taking any action. For such matters, you should seek advice from a qualified advisor regarding your specific circumstances.

No representations, warranties, or assurances (express or implied) are made regarding the accuracy or completeness of the information in this publication, and neither DTTL nor its member firms, affiliates, employees, or agents shall be liable or responsible for any loss or damage of any kind arising directly or indirectly in connection with persons relying on this publication. DTTL and each of its member firms, as well as their affiliates, are legally separate and independent entities.