DATA PROTECTION IN INTERNAL INVESTIGATIONS

Justification and Accountability under the GDPR

Dr. Jan-Michael Grages

European Privacy KnowledgeNet 2026

Munich, 12 October 2026

KNPZ

TOPICS AND TRIGGERS

- What subjects are investigated?
- Why are investigations initiated?



TOPICS AND TRIGGERS

Abbildung 74: Wachsende Themenkomplexe in Bezug auf interne Untersuchungen

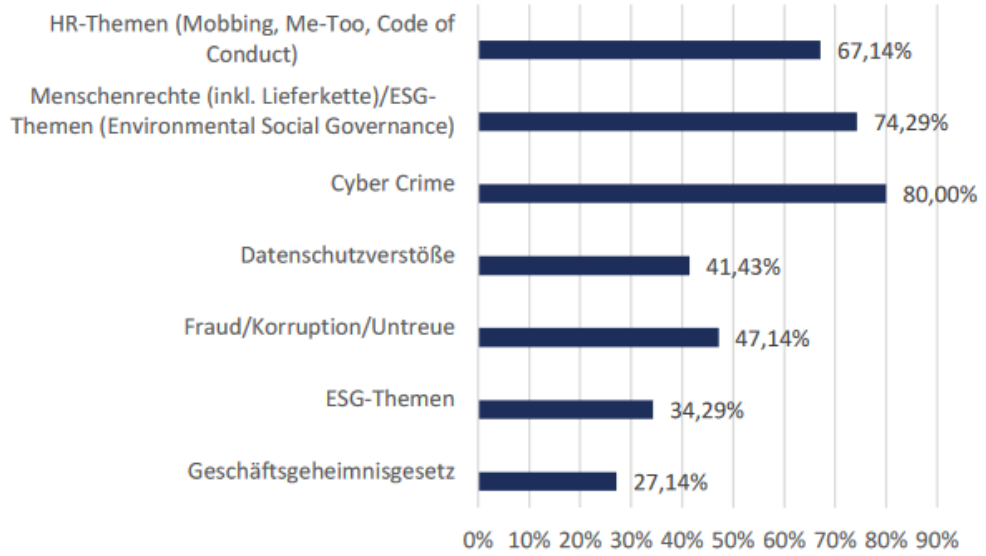
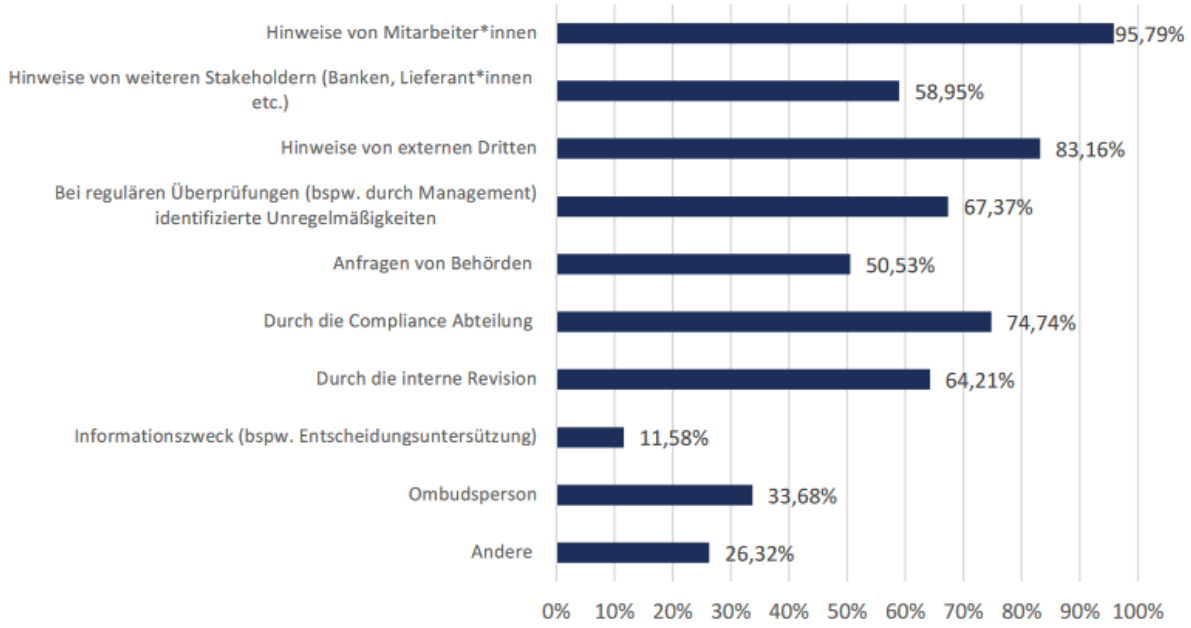


Abbildung 21: Auslöser von internen Untersuchungen



Source: German Institute for Compliance, DICO Study—Internal Investigations in Germany (2022), www.dico-ev.de

RELEVANCE AND CHALLENGES

Abbildung 69: Entwicklung der Anzahl der internen Untersuchungen in Unternehmen in den nächsten Jahren

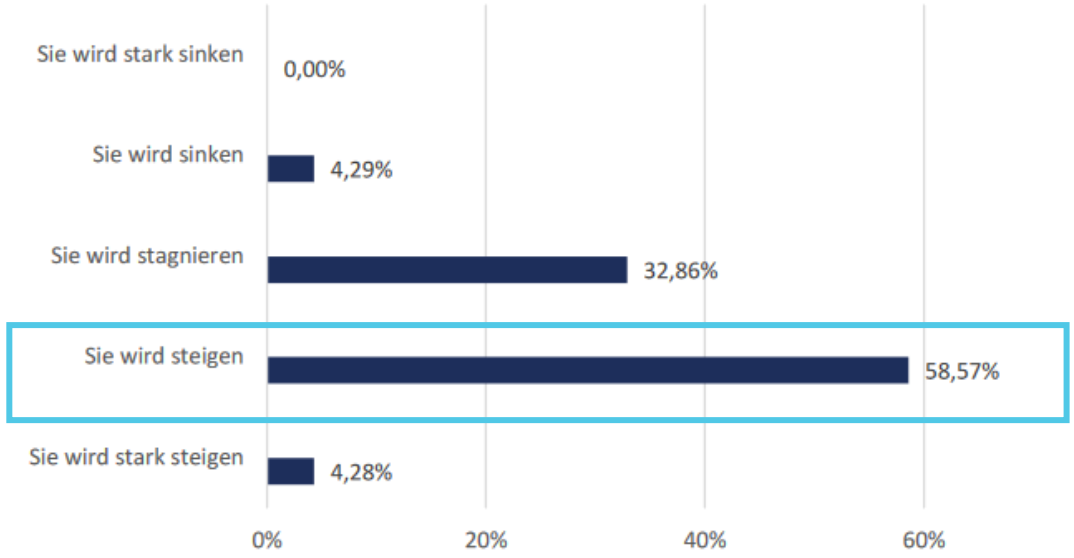
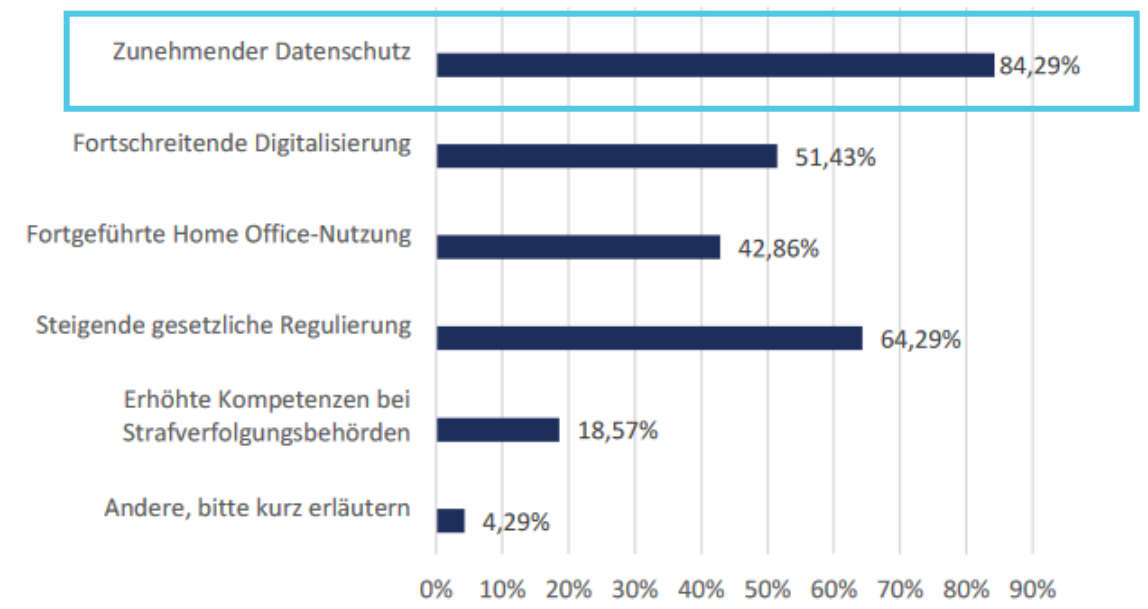


Abbildung 73: Herausforderungen in Bezug auf interne Untersuchungen in den nächsten drei Jahren



Mehrfachnennungen möglich

Source: German Institute for Compliance, DICO Study—Internal Investigations in Germany (2022), www.dico-ev.de

OBJECTIVES AND DATA PROTECTION RISKS

- Misconduct shall be investigated
  - Proactive measure (as opposed to or in addition to external investigations)
  - Distinction from preventive screenings
- What challenges arise?

▪ Legal basis for processing ▪ Accountability	→ Internal documentation Risk of fines (regulatory authorities)
▪ Notification of data subjects ▪ Handling of data subjects' rights	→ External communication Risk of damages (data subjects)

↳ Possible repercussions on external sanctions and internal options for action

AGENDA

- Presentation to establish legal toolbox
- Discussion of practical scenarios



SCENARIOS FOR AN INTERNAL INVESTIGATION



CEO Stealing Information



Working-Hour Fraud



Regulatory Violation



Cybersecurity Incident



Post-M&A Dispute

PROCEDURE

WHY IS AN INTERNAL INVESTIGATION CONDUCTED?

- Misconduct is addressed internally, e.g., via a whistleblower
- Misconduct is addressed externally, e.g., through the media
- Request from a regulatory authority to prevent or limit an external investigation

- What are the motivations

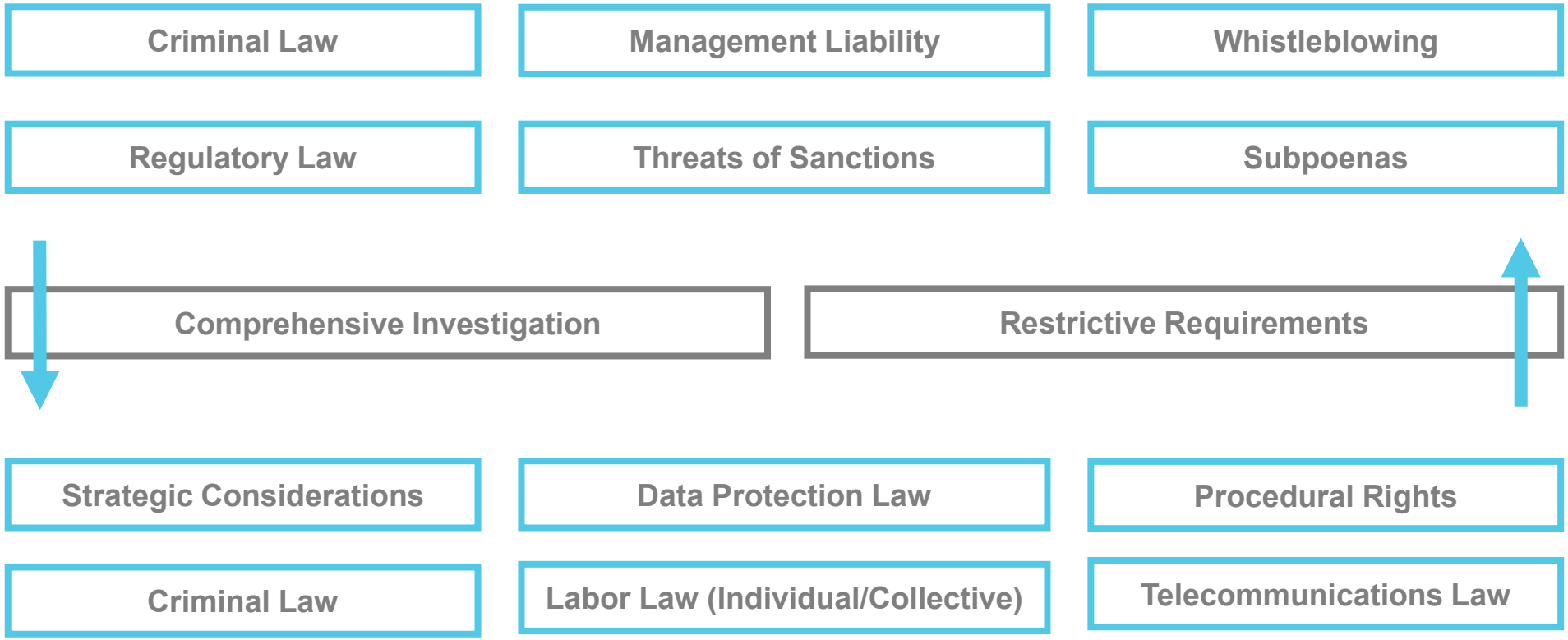


WHY IS AN INTERNAL INVESTIGATION CONDUCTED?

- Misconduct is addressed internally, e.g., via a whistleblower
- Misconduct is addressed externally, e.g., through the media
- Request from a regulatory authority to prevent or limit an external investigation

- Various motivations
  - Clarification and resolution of the problem
  - Mitigation of sanctions
  - Protection of reputation
  - Avoiding personal liability

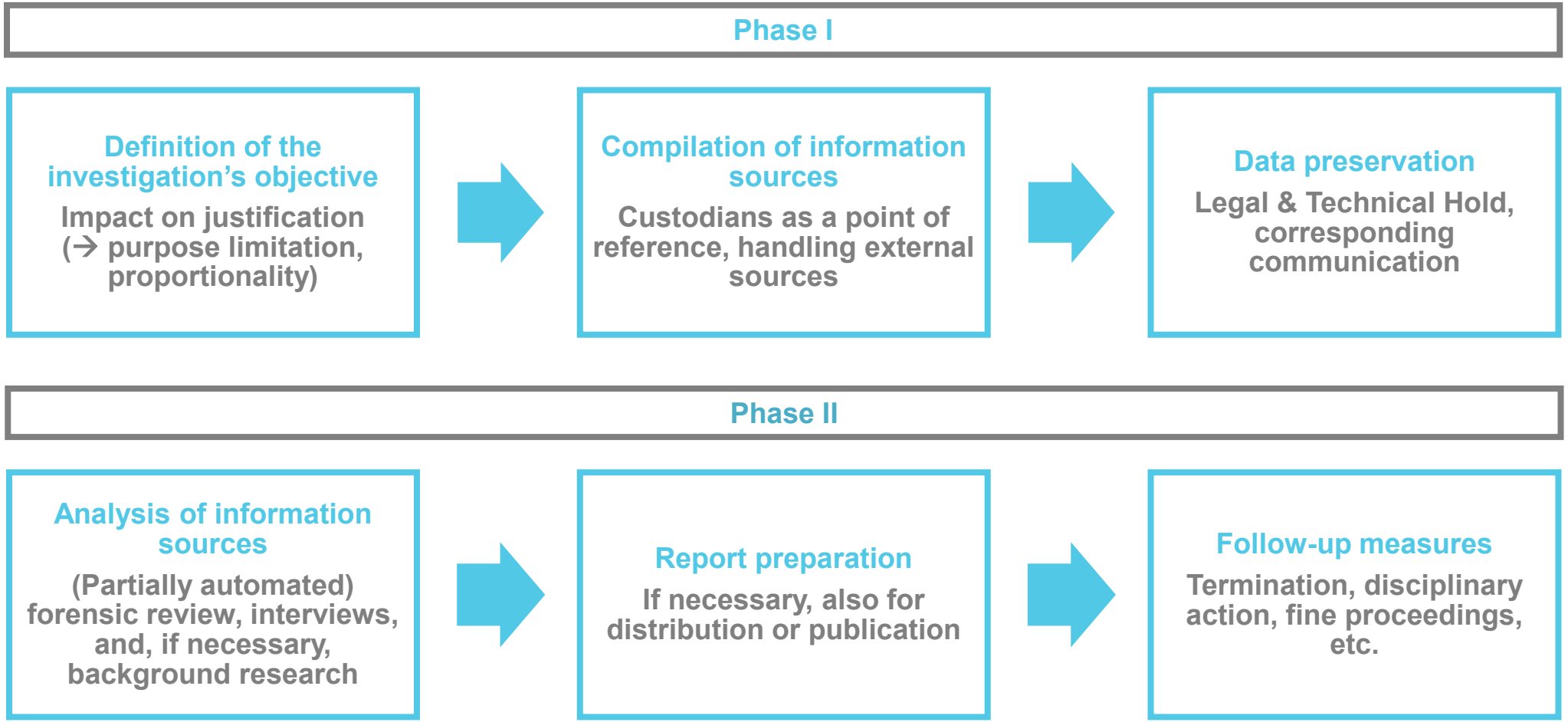
LEGAL COMPLEXITY



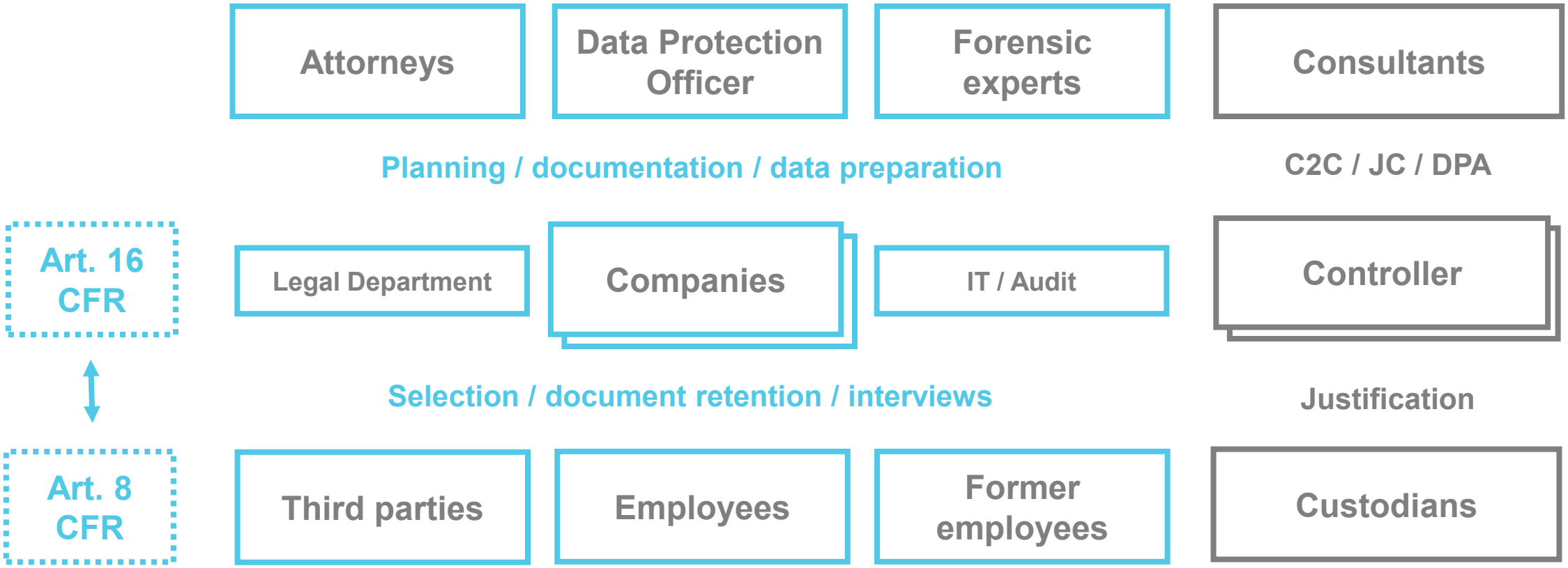
Typical of data protection law: balancing of interests rather than clear prohibitions or obligations

KNPZ RECHTSANWÄLTE

HOW DOES AN INTERNAL INVESTIGATION PROCEED?



WHO ARE THE STAKEHOLDERS?



KNPZ RECHTSANWÄLTE

JUSTIFICATION

RELEVANT PROCESSING ACTIVITIES

- Document review (→ handling of email and messenger/chat)
- Analysis of files/drives (→ handling of records)
- Documentation of interviews (→ informed consent and voluntary participation)
- Analysis of additional data sources (→ video recordings, time tracking, logs)

- Transfers between the parties (→ including, where applicable, disclosure to third parties)
- Compilation into a report (→ redaction)

JUSTIFICATION UNDER THE GDPR

- Art. 6(1)(a) GDPR: Consent vs. voluntary Participation, transparency, and investigative tactics
- Art. 6(1)(c) GDPR: Is there a “legal obligation”?
- Art. 6(1)(e) GDPR: Performance of a task carried out in the public interest?

- Art. 6(1)(b) GDPR: Performance of the employment or business relationship?
- Art. 6(1)(f) GDPR: Overriding interests vis-à-vis employees and third parties?

- Art. 6(4) GDPR: Is the purpose of the investigation compatible with the initial purposes of processing?

BALANCING OF INTERESTS (1/2)

- Factors in the balancing test
  - Degree of suspicion (→ documented initial suspicion that must be verified)
  - Clear definition of purpose (→ no “fishing expedition”)
  - Restrictive selection and storage of material (→ no shadow databases)
  - Removal of identifiability (→ difficulties due to job titles)

- Compatibility of purposes
  - Interconnection of purposes
  - Relationship between data subjects and the company
  - Type of data
  - Consequences of further processing
  - Encryption/pseudonymization

BALANCING OF INTERESTS (2/2)

- Justification for Disclosure
  - Affiliated companies
  - Attorneys and other independent advisors
  - Third countries (→ assertion of legal claims, Art. 49(1)(e) GDPR)
  - Government authorities (→ formal obligation vs. voluntary cooperation)

- Handling a “conflict of obligations”
  - Comparison of sanctions (→ GDPR’s fine range as a game-changer)
  - Impending prohibitions on the use of evidence

REQUIREMENTS

PROCEDURAL REQUIREMENTS

- Clarification of responsibilities and process flow
- Filtering steps to ensure data minimization
- Developing a specific data deletion strategy
- Anonymization/pseudonymization (→ redaction protocol)
- Ideally: align with existing guidelines (→ avoid change of purpose)

- Conduct a Data Protection Impact Assessment (→ high risk, standard process vs. ad hoc measure)
- Document the balancing of interests (→ Legitimate Interests Assessment)
- Transfer Impact Assessment (for transfers to third countries)

TRANSPARENCY REQUIREMENTS

- Starting point: Art. 13(3) and Art. 14(4) GDPR: Information regarding a change in purpose
  - Jeopardizing the objective of the investigation
  - Practical problems: effort and accessibility
- Reasons to avoid transparency



TRANSPARENCY REQUIREMENTS

- Starting point: Art. 13(3) and Art. 14(4) GDPR: Information regarding a change in purpose
  - Jeopardizing the objective of the investigation
  - Practical problems: effort and accessibility

- Exceptions
  - Factual impossibility (see Art. 14(5)(b) GDPR)
  - Confidentiality/professional secrecy
  - Assertion of legal claims

  → Public disclosure or retroactive compliance may be required

CREATING TRANSPARENCY

- Operational Implementation
  - Updates as the investigation progresses
  - Threshold for initiating investigations involving external parties and former employees
- Generic information as a line of defense
  - Reference to general data protection notices
  - Threshold for providing specific details
- Advantages and disadvantages of detailed information
  - Strengthening the balancing of interests
  - Management of data subjects' rights

↳ **Data protection information can be a form of corporate communication**

HANDLING REQUESTS FOR INFORMATION

- The right of access in practice
  - Lever for attack and obstruction (misuse and the ECJ)
  - Timing of the provision of information
  - Handling excessive requests (volume vs. scope)

  → To what extent must known data be disclosed?

  → To what extent must contextual information be disclosed?

- Exceptions to the right of access
  - Priority rights of third parties (see Art. 15(4) GDPR)
  - Protection of whistleblowers vs. rights of the reported party

↳ A generic response may serve as a first line of defense

The art of “salami tactics”

HANDLING OBJECTIONS

- The right to object in practice
  - Lever for attack and obstruction
  - Timing of the objection
  - → To what extent must the data subjects explain their position?
- Handling objections
  - Anticipating a subsequent balancing of interests
  - Considering time limit provisions
  - Objection should only prevail in exceptional cases

SCENARIOS

PERSPECTIVES - ENABLER VS. DATA PROTECTION ADVOCATE



Team Investigator



Team Challenger

RULES OF THE GAME

TEAM INVESTIGATOR

- Mandate: design fast and robust investigation
- Per scenario: name your first moves and the legal basis

TEAM CHALLENGER

- Mandate: stress-test every step
- Per scenario: raise an issue and a data subjects' right

SCENARIO 1 - THE EX-CEO AND THE TRADE SECRETS

FACTS:

The CEO left the company 10 days ago under tense circumstances. His company laptop, Outlook mailbox and MS Teams history are still on your systems. The CTO suspects the ex-CEO walked out with the product roadmap and the key customer list.

How far can you go without talking to him?

SCENARIO 1 - THE EX-CEO AND THE TRADE SECRETS

TEAM INVESTIGATOR

Protecting trade secrets after the CEO walked

- Preserve first, analyze second - image the laptop, mailbox and Teams archive today to stop tampering
- Legal basis Art. 6(1)(f) GDPR - concrete suspicion of a serious breach of post-contractual duties
- Narrow, keyword-based review - not a full content read, four-eyes principle on every hit
- Written scope memo - custodians, date range, keywords, reviewer tiers, retention clock
- In parallel - litigation hold, preservation notice, and review of NDA and non-compete

SCENARIO 1 - THE EX-CEO AND THE TRADE SECRETS

TEAM CHALLENGER

Where the review has to stop

- If private use of the mailbox was tolerated, private correspondence must be filtered out before any review
- Full forensic imaging is not necessary where targeted search would do
- Retention of the forensic copy must be time-limited and purged when the purpose ends
- Art. 14 GDPR duty towards third-party correspondents swept into the review
- LIA must be in writing before processing starts, not after

SCENARIO 1 - THE EX-CEO AND THE TRADE SECRETS

COMPLIANT APPROACH

What a defensible ex-CEO investigation looks like

- Preserve the forensic image under a documented hold, with a retention end-date
- Written scoping memo - custodians, keywords, date range, reviewer tiers, four-eyes principle
- Pre-review privacy filter where private mailbox use was tolerated
- Documented LIA on Art. 6(1)(f) GDPR before any content review
- Art. 14 GDPR information to third-party correspondents where it does not frustrate the purpose

SCENARIO 2 - SICK LEAVE AND THE SECOND JOB

FACTS:

A long-serving employee has been on sick leave for six weeks. A colleague reports seeing him working shifts at a competitor's shop. HR wants answers.

HR wants to hire a private investigator to film employee at the second job. Green-light?

SCENARIO 2 - SICK LEAVE AND THE SECOND JOB

TEAM INVESTIGATOR

Testing the sick-leave suspicion

- Document the suspicion in writing (what, when, who said it) before any processing step
- Least intrusive means first - shift logs, customer records, line-manager observations
- Open source check of public professional social media, with scope and keyword limits
- Legal basis Art. 6(1)(f) for a serious contractual breach, Art. 9 incidentally
- External surveillance only if evidence remains thin - narrow days and locations, written legal opinion

SCENARIO 2 - SICK LEAVE AND THE SECOND JOB

TEAM CHALLENGER

Why the private investigator is not the first move

- Sick-leave context pulls Art. 9 GDPR health data into every processing step → higher bar
- Covert surveillance is ultima ratio, concrete, documented suspicion is a precondition
- Private life must stay out of the report - data minimization on the deliverable
- Art. 13/14 notice to the employee - any delay must be justified in writing
- Open source monitoring is still processing - it needs a basis and a defined scope, no private social media

SCENARIO 2 - SICK LEAVE AND THE SECOND JOB

COMPLIANT APPROACH

The ultima-ratio ladder

- Written suspicion memo first (what, when, source)
- Internal data first → shift logs, customer records, line-manager observations
- Scoped open source check → public sources only, defined scope, no bystanders
- External surveillance only on a reasoned written legal opinion (narrow days and locations, tight retention)
- Minimize report data, Art. 9 health data only where unavoidable

SCENARIO 3 - WHAT WASN'T IN THE DATA ROOM

FACTS:

A PE fund closed the acquisition of a mid-cap target six months ago. A material product liability claim has just surfaced that the fund believes was known to the seller's management but was never disclosed in the data room.

You want to re-open the data room and read the former management's mailboxes to prove the claim was hidden. What's your legal basis?

SCENARIO 3 - WHAT WASN'T IN THE DATA ROOM

TEAM INVESTIGATOR

Running the dispute without breaking the target

- Review to build claim - fresh purpose, fresh Art. 6(1)(f) basis, fresh Art. 30 entry
- Ring-fence privileged DD advisor material → do not pull it into the general review set
- Prepare a position for the data subjects' rights you expect from former management
- EU-host the review platform, US transfers inside the PE group → only on SCCs plus TIA

SCENARIO 3 - WHAT WASN'T IN THE DATA ROOM

TEAM CHALLENGER

The DD data was not collected for this

- Purpose limitation (Art. 5(1)(b)) → DD data was collected for due diligence, not litigation
- Joint-controller analysis with the seller for pre-signing data
- Former management keep their data subjects' rights after they leave
- Cross-border transfers inside the PE group → Art. 44 ff., TIA requirement
- Target's own Art. 30 records must be updated to reflect the new processing purpose

SCENARIO 3 - WHAT WASN'T IN THE DATA ROOM

COMPLIANT APPROACH

Corporate processing done right

- Requirements similar to original due diligence exercise
- Privileged DD advisor material ring-fenced from the general review set
- Intra-group transfers on SCCs plus TIA, EU-hosted review platform
- Deferral note to data subjects prepared in advance

SCENARIO 4 - ANTITRUST: 50 CUSTODIANS, ONE WEEK

FACTS:

Credible evidence suggests a group of your sales employees coordinated prices with competitors. A dawn raid is possible next week. You have ~50 custodians to review, half of whom are in contact with competitors.

You need to prepare for the raid and run an internal review at the same time. Where do you start?

SCENARIO 4 - ANTITRUST: 50 CUSTODIANS, ONE WEEK

TEAM INVESTIGATOR Coordination of raid and processing

- Written scoping on day 1 → custodian list, date range, keyword list, reviewer tiers
- EU-hosted review platform (lawyer-only review tier for privileged custodians)
- Art. 28 DPA with the e-discovery provider
- Ring-fence privileged material from the outset, separate reviewer pool
- Parallel raid protocol (door, interview, imaging, employee communication)
- Deferral note to data subjects prepared in advance

SCENARIO 4 - ANTITRUST: 50 CUSTODIANS, ONE WEEK

TEAM CHALLENGER

A mass review is a mass processing

- Mass custodian review needs heightened proportionality under Art. 6(1)(f)
- Third-party and competitor personal data swept into the review → their rights also apply
- Art. 15 claims cannot be dropped → any deferral must be reasoned and time-limited
- International transfers to US e-discovery platforms → SCCs plus TIA
- Art. 33/34 apply if the review itself discovers a separate personal data breach

SCENARIO 4 - ANTITRUST: 50 CUSTODIANS, ONE WEEK

COMPLIANT APPROACH

Raid-ready and GDPR-defensible

- Written scoping on day 1 (custodians, dates, keywords, reviewer tiers)
- EU-hosted platform, lawyer-only review tier for privileged custodians, Art. 28 DPA
- Separate reviewer pool for privileged material, privilege log maintained
- Deferral note to data subjects prepared in advance
- Art. 33/34 workflow ready if the review surfaces a separate breach

SCENARIO 5 - 72 HOURS TO CURE THE BREACH

FACTS:

Alerts suggest an insider helped a threat actor move laterally through your network. The exfiltration window is still open. You want to analyze VPN logs, badge data, and the full employee directory to reconstruct the path.

72 hours on the clock. How to run the analytics?

SCENARIO 5 - 72 HOURS TO CURE THE BREACH

TEAM INVESTIGATOR

Analytics without losing the 72 hours

- Contain first → analytics run in parallel on log sources
- Legal basis Art. 32 GDPR (security duty) and/or Art. 6(1)(f) for the specific investigation
- Art. 28 DPA with the forensic service provider (agreed scope of data access)
- DPIA template for forensic analytics on file, updated for this incident
- Notify under Art. 33 with the information you have, update later under Art. 33(4)
- Written retention plan for forensic datasets (purpose, period, deletion or anonymization)

SCENARIO 5 - 72 HOURS TO CURE THE BREACH

TEAM CHALLENGER

Security is a basis, not a blank cheque

- Log analysis of employee activity needs explicit limits → no behavioral profiling (Art. 22)
- DPIA required under Art. 35 when the analytics scale to behavioral inference
- Transfers to forensic service provider outside the EEA → SCCs and TIA
- Processor controls under Art. 28 → what the forensic service provider sees, keeps, and deletes
- Forensic datasets cannot live forever → defined retention and purge
- Art. 34 notice to individuals must be timely and meaningful

SCENARIO 5 - 72 HOURS TO CURE THE BREACH

COMPLIANT APPROACH

72 hours with legal basis sorted up-front

- Pre-prepared playbook that lists authorized log sources and analytics
- Pre-prepared DPIA (Art. 35) kept current and updated for each incident
- Pre-signed Art. 28 DPA with the forensic service provider, defined scope of data access
- Art. 33 notification with the information you have, update later under Art. 33(4)
- No behavioral profiling of employees → scope limits in writing
- Retention and purge plan for forensic datasets

THREE RULES TO SUM IT UP

1

LEGAL BASIS IS A TWO-STEP

Investigation purpose in each specific processing step (collection, review, transfer, retention)

2

DOCUMENTATION IS THE COMPLIANCE

If it is not written down, it did not happen

3

DATA SUBJECTS' RIGHTS DO NOT PAUSE

Have a defensible position ready before the first data subjects' right lands

THANK YOU

KNPZ
RECHTSANWÄLTE

Your Contact

Dr. Jan-Michael Grages
Partner, Attorney at Law
grages@knpz.de

KNPZ Rechtsanwälte Partnerschaftsgesellschaft mbB
Kaiser-Wilhelm-Straße 9, 20355 Hamburg
Phone +49 40 63607590
www.knpz.de

