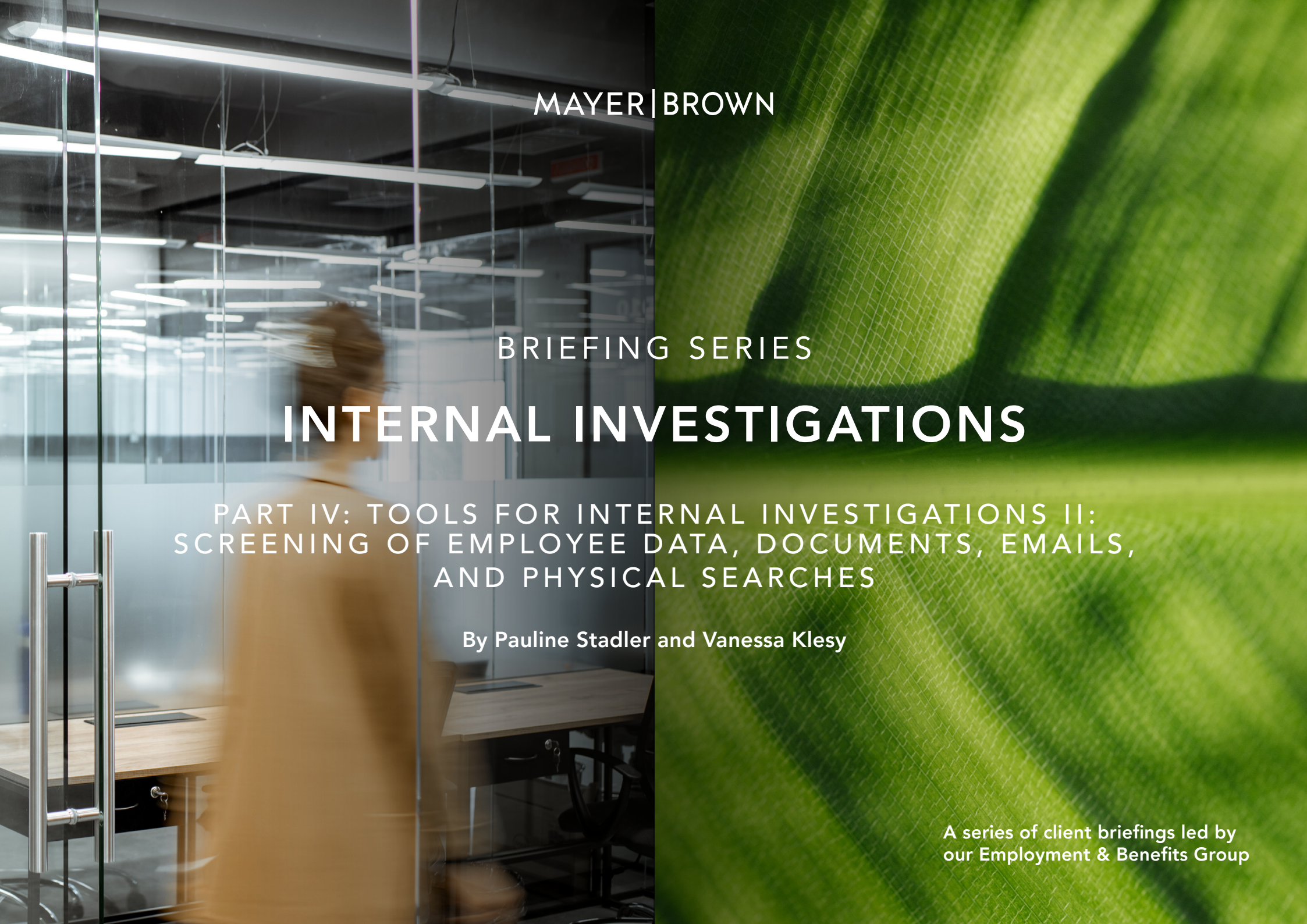


MAYER|BROWN

BRIEFING SERIES

INTERNAL INVESTIGATIONS

PART IV: TOOLS FOR INTERNAL INVESTIGATIONS II: SCREENING OF EMPLOYEE DATA, DOCUMENTS, EMAILS, AND PHYSICAL SEARCHES

By Pauline Stadler and Vanessa Klesy

A series of client briefings led by our Employment & Benefits Group

This Part IV of our Briefing Series explains how companies can lawfully and effectively screen employee data, documents, and emails, and how to conduct proportionate physical searches in a manner that is defensible and operationally practical.

The core message is straightforward: screening measures and searches must be purposedriven and proportionate, based on a valid legal ground under data protection law, and compliant with additional constraints that may arise where private use of company systems is permitted or where telecommunications secrecy or deviceaccess rules apply.

In Germany, the relevant legal framework is anchored in the General Data Protection Regulation (*GDPR*), the German Federal Data Protection Act (Bundesdatenschutzgesetz – *BDSG*), and the Telecommunications and Digital Services Data Protection Act (Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz – *TDDDG*), and the Telecommunications Act (Telekommunikationsgesetz – *TKG*) in certain scenarios.

Wherever possible, companies should favor transparent and open investigative measures and refrain from covert actions unless there is a documented suspicion of a criminal offense and no less intrusive means are available.

For interviewbased factfinding, see **Part III** of our Briefing Series. Guidance on governance structures, reporting lines, and decision rights is set out in **Part II**. A detailed discussion of legal bases, datasubject rights, and the exclusionofevidence doctrine follows in **Part V.**

WHAT'S INSIDE

SCOPE AND GUIDING PRINCIPLES FOR SCREENING AND SEARCHES

Employee data screening and workplace searches should be narrowly scoped to answer clearly defined investigative questions and must adhere to the principles of necessity, data minimization, and purpose limitation. As a default, companies should proceed in an open and transparent manner, with clear notice to affected employees and a documented plan setting out what is being searched, why the measure is necessary, and how confidentiality is safeguarded and the use of personal data limited.

The GDPR's core processing principles apply in full, including lawfulness, fairness, and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability. The accountability principle, in particular, requires controllers not only to comply with these standards but to be able to demonstrate compliance through appropriate documentation, decisionmaking records, and technical and organizational controls.

Broad, ongoing, or covert monitoring without a specific investigative purpose or concrete factual triggers is impermissible and carries a significant risk of unlawful processing and the exclusion of evidence. Under established German practice, surveillance measures must be limited in scope, targeted to the concrete suspicion, and timebound. In ordinary operations, employees must be informed about the nature, scope, and purpose of any monitoring. Covert measures are reserved for exceptional cases, typically involving suspected criminal conduct, and only where less intrusive alternatives have proven insufficient. These requirements reflect the constitutional right to informational selfdetermination and the proportionality test embedded in GDPR and BDSG practice.

Companies should also plan carefully for transparency obligations and their narrowly defined exceptions. While Articles 13 and 14 GDPR generally require information to be provided to data subjects, Section 33 BDSG permits limited deviations in exceptional circumstances, including where providing information would jeopardize the establishment, exercise, or defense of civil claims or would undermine the purpose of processing for the prevention or investigation of criminal offenses. Any reliance on these exceptions must be assessed on a casebycase basis, balanced against data subject interests, and thoroughly documented.

Finally, a data protection impact assessment (DPIA) is required where processing is likely to result in a high risk to employees' rights and freedoms. This will typically be the case for systematic monitoring, largescale processing, datalossprevention tools with profiling functionality, geolocation of employees, or the deployment of novel or intrusive technologies. In practice, whistleblower systems and many technical surveillance measures will regularly trigger DPIA obligations.

KEY TAKEAWAYS

- **Purpose first:** Screening and searches must be narrowly defined, necessary, and proportionate.
- **Transparency as default:** Open measures with clear notice and documentation are the rule.
- **No fishing expeditions:** Broad, continuous, or untargeted monitoring is generally impermissible.
- **Covert measures are exceptional:** Only permissible where there is a documented suspicion of criminal conduct and no less intrusive means.
- **Observe information duties:** Articles 13/14 GDPR apply; Section 33 BDSG exceptions are narrow and must be carefully documented.
- **Check DPIA early:** Systematic monitoring, whistleblower tools, or intrusive technologies often trigger DPIA obligations.

LEGAL BASES AND EVIDENTIARY CONSEQUENCES

Employee data screening and workplace searches must be grounded on a valid legal basis. In the German employment context, processing will typically rely on Article 6 GDPR, read in conjunction with Article 88 GDPR and the applicable national implementing rules.

Historically, Section 26 BDSG has provided a specific employmentlaw legal basis, anchored in the concept of "necessity" for purposes related to hiring, performance of the employment relationship, and termination, complemented by a distinct provision for the detection of criminal offenses. Following the ECJ's judgment of 30 March 2023, which clarified the conditions under which national employmentdata rules remain permissible under Article 88 (2) GDPR, courts and commentators increasingly emphasize that the GDPR prevails wherever national provisions fail to meet Article 88 requirements. Against this background, a prudent approach is to frame processing primarily under Article 6 GDPR, while observing Section 26 BDSG where applicable and documenting necessity and proportionality with particular rigor.

The crimedetection pathway remains a narrow exception subject to strict conditions. Under Section 26 (1), sentence 2 BDSG, employers must be able to demonstrate (i) documented and factual indications of a criminal offense committed in the employment context, (ii) that the chosen measure is necessary and proportionate to detect the offense, and (iii) that the employee's legitimate interests do not outweigh the employer's interests, taking into account the nature and scope of the measure. Less intrusive alternatives must be considered and exhausted first.

In addition, employers must respect purpose limitation and purposechange rules. The reuse of lawfully collected employee data for investigative purposes may require a separate legal basis and a documented purposechange assessment. This may include reliance on Section 24 BDSG for processing necessary to assert, exercise, or defend civil claims, combined with appropriate safeguards such as pseudonymization or encryption.

Finally, companies should anticipate admissibility risks. German labor courts recognize that serious dataprotection or privacy violations may lead to the exclusion of evidence, particularly where constitutional rights are affected. Even lawfully obtained data must be evaluated in a manner consistent with the original processing purpose. While violations of codetermination requirements or internal policies alone do not automatically render evidence inadmissible, unlawful data collection can do so, following a casebycase constitutional balancing.

LEGAL BASIS & EVIDENCE – KEY POINTS

- **Article 6 GDPR as the anchor:** Frame screening and searches primarily under the GDPR; apply Section 26 BDSG with caution postECJ (30 March 2023).
- **Section 26 BDSG crime exception is narrow:** Requires documented suspicion, necessity, proportionality, and exhaustion of milder means.
- **Mind purpose limitations:** Reuse of existing data may trigger a purposechange assessment and a new legal basis (e.g. Section 24 BDSG).
- **Document proportionality carefully:** Legal basis, balancing, and safeguards should be recorded in detail.
- **Evidence at risk:** Serious privacy violations can lead to exclusion of evidence in labor court proceedings.

DIGITAL SOURCES AND INVESTIGATION PATHWAY

Most investigations start with company data. The investigation pathway should follow a **"businessfirst" and minimally invasive approach**. Employers should initially focus on clearly businessrelated repositories such as shared drives, documentmanagement systems, collaboration platforms, ticketing or CRM systems, and audit or access logs. Only where these sources do not sufficiently answer the investigative questions, and where justified by necessity and proportionality, should companies move on to individual mailboxes, endpoint imaging, or mobile device data.

EMAIL AND MESSAGING

Where private use of company systems is expressly prohibited and effectively enforced, employers may review business communications in line with necessity and proportionality, provided that blanket or permanent monitoring is avoided. Where private use is permitted or tolerated, access must be handled with particular caution.

Whether allowing private use triggers telecommunications secrecy obligations under the TDDDG/TKG remains a contested issue in Germany. However, there is a significant body of authority — including several data protection supervisory authorities — taking the restrictive view that private use subjects employers to telecommunications secrecy, which would prohibit access to communication content except under narrow statutory exceptions. Although some commentators argue that Section 3 TDDDG does not apply to employers even in private-use scenarios, companies should not rely on the more permissive interpretation without careful legal assessment. Given the severity of the potential consequences — including criminal liability under Section 206 of the German Criminal Code (Strafgesetzbuch — *StGB*) and the risk of evidence being excluded in court — employers who permit private use should, as a matter of prudence, refrain from screening email content unless they can demonstrate compliance with telecommunications secrecy requirements or have implemented robust measures to separate private from business communications.

In practice, riskmitigating measures are essential: employers should favor traffic data and logs over content review, apply tight temporal scopes, sender/recipient filters, and keyword limitations, and ensure that clearly private communications are excluded. A casespecific balancing of interests should be documented.

DOCUMENTS AND COLLABORATION TOOLS

Modern collaboration suites can generate analytics that indirectly monitor employee behavior or performance. Employers should rely on aggregated or rolebased insights, restrict access on a strict needtoknow basis, and disable or limit profilingtype features unless a valid legal basis exists. Where tools are capable of monitoring performance or behavior, works council codetermination under Section 87 (1) no. 6 Works Constitution Act (Betriebsverfassungsgesetz – *BetrVG*) is typically required, with guardrails documented in a works agreement.

ENDPOINTS AND KEYLOGGERS

Targeted imaging of laptops or the collection of specific folders may be permissible where necessary and proportionate. By contrast, keyloggers, continuous screen capture, or similar "total surveillance" tools are generally unlawful, absent a concrete suspicion of a criminal offense or serious breach—and even then only if narrowly tailored. German courts have repeatedly rejected evidence obtained through keylogging without a concrete suspicion.

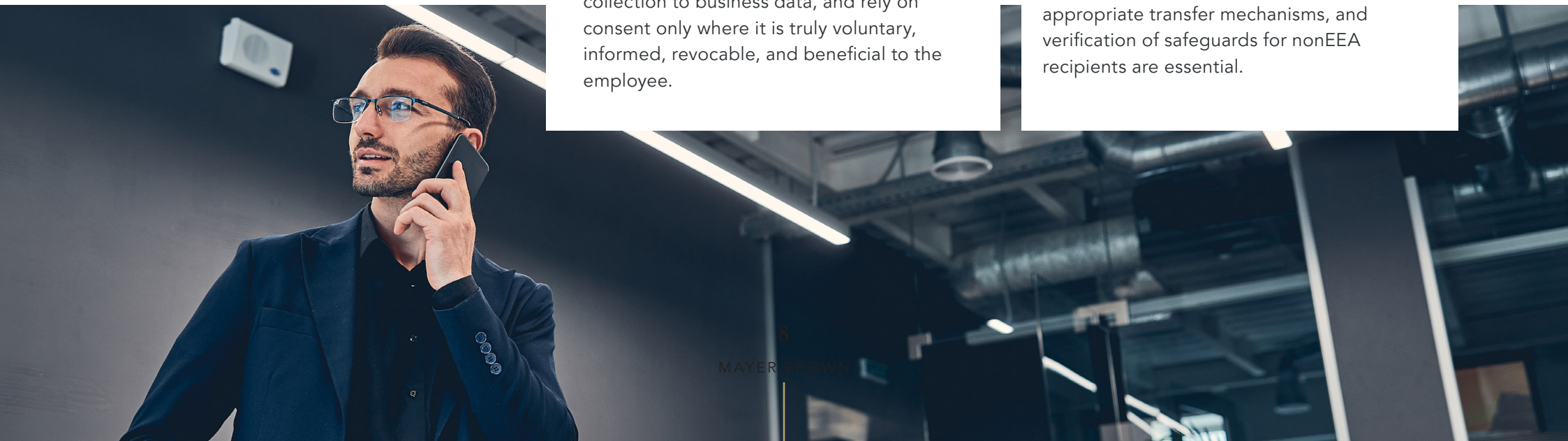
MOBILITY AND GPS

Tracking company vehicles or devices may be permissible during working hours for defined operational or safety purposes, but not during breaks or offduty time. For safetycritical roles or asset protection, limited GPS tracking may be justified under Article 6 (1) (f) GDPR or, in narrow cases, Section 26 BDSG, provided tracking is strictly confined to working time.

Bring-Your-Own-Device (BYOD) scenarios require particular care. A robust setup should separate personal and business data through mobiledevicemanagement solutions, limit collection to business data, and rely on consent only where it is truly voluntary, informed, revocable, and beneficial to the employee.

PROCESS HYGIENE

Sound process design is critical. Employers should provide clear notices in policies or works agreements, limit access to investigation data to a needtoknow circle, and log all searches, queries, and exports. Where investigations involve systematic monitoring, datalossprevention tools, or geolocation, a Data Protection Impact Assessment (DPIA) will often be required pursuant to Article 35 GDPR. For processors and crossborder transfers, Article 28 GDPR agreements, appropriate transfer mechanisms, and verification of safeguards for nonEEA recipients are essential.



PHYSICAL SEARCHES, CCTV, AND SENSITIVE ZONES

Physical searches should be rare, risk-based, and framed by policy or works agreements. Random, announced bag checks at store exits or controlled access to restricted areas can be permissible if proportionate, nondiscriminatory, and transparently communicated. Lockers, desks, and other company property may be inspected where necessary for defined purposes and in a manner that minimizes intrusion, for example in the presence of a witness and with the employee invited to attend if feasible. Private belongings require consent or strong, documented grounds in exceptional cases.

Video surveillance must be purpose limited and confined to justified areas such as entrances, high-risk zones, or cash points. Cameras are prohibited in locations with a high expectation of privacy, such as changing rooms and sanitary facilities, and covert CCTV is restricted to exceptional crime-detection cases backed by concrete suspicion and as a last resort. Employers should provide clear signage where cameras operate, define retention periods as short as possible, and evaluate footage only when a legitimate reason arises. Assess legal bases cumulatively across affected persons. For employees, Section 26 BDSG and Article 6 GDPR may both need to be examined; for non-employees, rely on Article 6 GDPR.

For searches that intersect with interviews or disciplinary steps, maintain the separation between fact-finding and decision-making described in Part II, and align with the fair-interview practices in Part III. Preserve chain of custody and document necessity at each step to mitigate evidentiary exclusion risks.

WORKS COUNCIL CO-DETERMINATION AND DATA-SHARING BOUNDARIES

Physical searches should be rare, risk-based, and framed by policy or works agreements. Random, announced bag checks at store exits or controlled access to restricted areas can be permissible if proportionate, nondiscriminatory, and transparently communicated. Lockers, desks, and other company property may be inspected where necessary for defined purposes and in a manner that minimizes intrusion, for example in the presence of a witness and with the employee invited to attend if feasible. Private belongings require consent or strong, documented grounds in exceptional cases.

Video surveillance must be purpose limited and confined to justified areas such as entrances, high-risk zones, or cash points. Cameras are prohibited in locations with a high expectation of privacy, such as changing rooms and sanitary facilities, and covert CCTV is restricted to exceptional crime-detection cases backed by concrete suspicion and as a last resort. Employers should provide clear signage where cameras operate, define retention periods as short as possible, and evaluate footage only when a legitimate reason arises. Assess legal bases cumulatively across affected persons. For employees, Section 26 BDSG and Article 6 GDPR may both need to be examined; for non-employees, rely on Article 6 GDPR.

For searches that intersect with interviews or disciplinary steps, maintain the separation between fact-finding and decision-making described in Part II, and align with the fair-interview practices in Part III. Preserve chain of custody and document necessity at each step to mitigate evidentiary exclusion risks.

PROCESS, DOCUMENTATION, AND INTERNATIONAL ALIGNMENT

Investigative screening should run on a written plan that states purpose, scope, legal basis, roles, and timelines, and that records key necessity and proportionality judgments. Where crime detection is invoked, document the specific indications, the narrower alternatives considered and rejected, and why the chosen measure is the last resort. Maintain a chain of custody for collected data, control access tightly, and use defensible deletion schedules. Anticipate evidence-admissibility risks. Severe violations can lead to exclusion of evidence, and courts will conduct constitutional balancing to determine use; violations of co-determination alone do not mandate exclusion, but unlawful acquisition can.

For multinational groups of companies, align global protocols with German specifics. Across jurisdictions, keeping monitoring targeted, transparent, and time bound is the most portable defense.

DOS AND DON'TS FOR SCREENING AND SEARCHES

Do

Define a specific purpose and legal basis for each measure, and record your necessity and proportionality analysis

Prefer business repositories and targeted queries before moving to personal mailboxes or endpoint imaging

Prohibit private use of company email and internet to avoid telecommunications-secrecy traps, or narrowly define monitoring in a works agreement where private use is allowed

Use open CCTV with clear signage, short retention, and focused placement, and never in sensitive areas

Secure works council co-determination for monitoring-capable systems and codify guardrails in a works agreement

Invoke crime-detection processing only with concrete, documented indications, after less intrusive means have failed

Apply DPIA and security-by-design, restrict access, log queries, and use proper processor contracts and transfer tools

Don't

Launch broad, continuous, or covert monitoring without a concrete purpose or documented suspicion

Collect "everything" from endpoints or mailboxes as a first step, or retain data longer than necessary

Access private communications content or metadata where private use is allowed, absent a narrow statutory basis and strict minimization

Place cameras in changing rooms or sanitary areas, or run covert CCTV without concrete suspicion and last-resort justification

Roll out monitoring features in IT systems without works council approval where co-determination applies

Use keyloggers or "total capture" tools in the absence of specific suspicion of crime or serious misconduct

Share data with vendors or affiliates without Article 28 agreements or appropriate cross-border safeguards

PRACTICAL TAKE-AWAYS FOR LEGAL, HR, AND COMPLIANCE

Build a structured monitoring and searches playbook. Define clear investigative pathways that begin with business repositories and escalate only where necessary. Embed the principles of necessity and proportionality at every stage, and include practical templates for purpose statements, legalbasis memoranda, balancing tests, and (where applicable) crimedetection documentation.

Clarify privateuse policies and codify guardrails. Decide whether private use of company communication systems is prohibited or permitted. Where private use is allowed, clearly define limits and monitoring parameters in IT policies and works agreements, recognizing both the heightened restrictions on accessing private content and the unresolved interplay between GDPR/BDSG and TDDDG/TKG.

Secure workscouncil approvals early. Most systems capable of monitoring employee behavior or performance trigger codetermination rights. Use works agreements to define purposes, data categories, access roles, retention periods, and reporting obligations, thereby reducing operational friction and legal risk. See **Part VI** for a detailed discussion of participation rights.

Avoid covert or continuous surveillance tools. Keyloggers, continuous screen capture, and blanket content reviews are generally impermissible and may only be considered as a last resort where there is a documented, concrete suspicion of criminal conduct. Wherever possible, rely on open, targeted, and timelimited measures.

Plan CCTV selectively and lawfully. Limit cameras to clearly justified areas, ensure visible signage, short and defined retention periods, and documented purposes, and exclude all sensitive locations. Footage should only be reviewed when a legitimate trigger arises, bearing in mind that even lawfully captured data requires a fresh proportionality and purpose assessment before use.

Protect evidence integrity and admissibility. Maintain a clear chain of custody, restrict access on a needtoknow basis, and align retention strictly with the investigative purpose. Employers should anticipate that unlawfully obtained data may be excluded by labor courts, potentially undermining disciplinary or termination measures. See Part V of our Briefing Series for dataprocessing requirements and exclusionofevidence risks.

TALK TO US

COUNSEL
VANESSA KLESY
EMPLOYMENT & BENEFITS
FRANKFURT +49 69 7941 1283
VKLESY@MAYERBROWN.COM

ASSOCIATE
PAULINE STADLER
EMPLOYMENT & BENEFITS
FRANKFURT +49 69 7941 2234
PSTADLER@MAYERBROWN.COM

MAYER | BROWN

MAYERBROWN.COM

AMERICAS | ASIA | EMEA

Mayer Brown is a leading international law firm positioned to represent the world's major corporations, funds, and financial institutions in their most important and complex transactions and disputes.

Please visit mayerbrown.com for comprehensive contact information for all our offices.

Mayer Brown is a global legal services provider comprising associated legal practices that are separate entities, including Mayer Brown LLP (Illinois, USA), Mayer Brown International LLP (England & Wales), Mayer Brown Hong Kong LLP (a Hong Kong limited liability partnership) and Tauil & Chequer Advogados (a Brazilian law partnership) (collectively, the "Mayer Brown Practices"). The Mayer Brown Practices are established in various jurisdictions and may be a legal person or a partnership. PK Wong LLC ("PKW") is the constituent Singapore law practice of our licensed joint law venture in Singapore, Mayer Brown PK Wong Pte. Ltd. More information about the individual Mayer Brown Practices and PKW can be found in the Legal Notices section of our website. "Mayer Brown" and the Mayer Brown logo are the trademarks of Mayer Brown. © 2026 Mayer Brown. All rights reserved.

Attorney Advertising. Prior results do not guarantee a similar outcome.