TERAMIND

Privacy Considerations for Teramind's User Activity Monitoring (UAM) Solution

This white paper is intended for informational purposes only and does not constitute legal advice. Organizations should consult with legal professionals to assess their specific legal obligations and compliance requirements.

In today's privacy-forward business climate, the implementation of User Activity Monitoring (UAM) software presents novel questions, particularly concerning compliance with privacy laws such as the General Data Protection Regulation (GDPR) in the European Union (EU) and relevant regulations in the United States (US).

As privacy professionals, it is imperative to understand and address these considerations to ensure that UAM software adoption respects employee rights while serving its intended purpose. Teramind is committed to helping its customers with a privacy-forward UAM solution deployment.

What does the US privacy regulatory landscape look like?

In the US, the expectation of privacy for employees and contractors in the workplace is limited, particularly when using company-owned devices or accessing company networks. Courts have generally held that employees and contractors have a reduced expectation of privacy in the workplace due to the employer's legitimate interests in maintaining productivity, security, and compliance. Multiple factors come into play when looking at the US regulatory landscape:

Fragmented legal framework:

The privacy law landscape in the US is characterized by a patchwork of federal and state laws, as well as regulations and enforcement actions by various government agencies. Unlike the EU with the GDPR, the US does not have a comprehensive, overarching federal privacy law that governs all aspects of data protection. Instead, privacy laws in the US are sector-specific and vary depending on the type of data and the industry involved. It's important to be mindful of some federal and state laws that provide specific protections for certain types of employee communications or activities, such as the Electronic Communications Privacy Act (ECPA), Wiretap Act, Stored Communications Act (SCA), and state laws governing electronic surveillance.

Company policies and contracts:

Employers often establish policies, such as acceptable use policies and employee handbooks, that outline the extent of privacy expectations in the workplace. Employees and contractors may have a reasonable expectation of privacy to the extent that these policies establish it. However, these policies typically reserve the right for the employer to monitor and access employee communications and activities conducted on company-owned devices or networks.

Notice:

Employers may provide notice to employees and contractors regarding monitoring in the workplace. This notice can serve to diminish the expectation of privacy by informing individuals that their activities may be monitored or recorded while using company resources. Notice may take the form of a disclosure in an employee handbook, a lock screen on a company-owned device indicating that this device is enrolled in monitoring, or other forms of disclosure. Courts have generally held that employees and contractors have a reduced expectation of privacy when using company-owned devices or accessing company networks.

There have been several political pushes for a federal privacy bill to harmonize the US privacy landscape and to bring the US regulatory environment closer to its EU counterpart. Absent federal preemption, numerous US States have spearheaded privacy legislation, substantially inspired by the GDPR. The first mover here was California, with the California Consumer Privacy Act (CCPA), as amended to the California Privacy Rights Act (CPRA). As of March 2024, the following US States will have a State privacy law in place:

- Florida (effective July 1, 2024)
- Oregon (effective July 1, 2024)
- Texas (effective July 1, 2024)
- Montana (effective Oct. 1, 2024)
- Delaware (effective Jan. 1, 2025)
- Iowa (effective Jan. 1, 2025)
- Tennessee (effective Jan. 1, 2025)
- New Jersey (effective Jan. 15, 2025)
- Indiana (effective Jan. 1, 2026)

What does the European privacy regulatory landscape look like?

In contrast to the US, the EU's GDPR harmonizes the privacy regulatory landscape in the EU. The GDPR applies across all EU Member States. Post-Brexit in 2018, the UK has adopted a national law that substantially tracks the EU GDPR, conveniently called the "UK GDPR". Local employment law considerations may tweak certain privacy law considerations (more on that below), but these baseline principles will apply across Europe:

- **Lawfulness, Fairness, and Transparency:** Data processing has to be lawful, fair, and transparent. Employers implementing UAM software should ensure that employees are informed about these activities, including the purposes of monitoring, types of data collected, and any rights they may have regarding their personal data.

TERAMIND PRO TIP:
Transparency measures are company and context-specific. For some inspiration, see the Notice Section.

- **Purpose Limitation:** UAM software should only collect and process employee data for specified, explicit, and legitimate purposes. Employers must clearly define the purposes of monitoring, such as ensuring security, enforcing company policies, or improving productivity, and ensure that data collected is not used for unrelated purposes.

TERAMIND PRO TIP:
Teramind's UAM software gives you a granular set of controls to customize your UAM deployment. For more information, see here:
https://www.teramind.co/product/teramind-uam

- **Data Minimization:** Employers should minimize the collection of personal data to what is necessary for the intended purposes. UAM software should only capture data relevant to monitoring activities, avoiding the collection of unnecessary personal information.

TERAMIND PRO TIP:
Teramind's UAM software allows you to create role-based access control as appropriate for your organization.

- **Individual Rights:** Employees have rights regarding their personal data under privacy laws, including the right to access, rectify, and erase their data. Employers must provide mechanisms for employees to exercise these rights concerning data collected through UAM software, ensuring transparency and accountability in data processing practices.

TERAMIND PRO TIP:
Organization admins have the option of downloading information for the purposes of honoring data subject access requests.

- **Cross-Border Data Transfers:** For companies operating in the EU and transferring employee data to jurisdictions outside the EU, such as the US, additional considerations arise regarding data transfer mechanisms, such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs), to ensure compliance with GDPR requirements for international data transfers.

TERAMIND PRO TIP:
Teramind offers a variety of deployment options to address the customer's unique geographic footprint and international data transfer compliance setup. For more information about Teramind's deployment options, please visit:

See On-Premises Deployments | See AWS Deployments

See Cloud Deployments | See Azure Deployments

- **Legal Basis for Processing:** Under the GDPR, employers must establish a lawful basis for processing employee data, such as consent, legitimate interests, or compliance with legal obligations. When implementing UAM software, employers should identify the appropriate legal basis for monitoring activities and document their reasoning to demonstrate compliance with privacy laws.

TERAMIND PRO TIP:
We've prepared a checklist for picking the most appropriate legal basis for you here.

- **Cross-Border Data Transfers:** For companies operating in the EU and transferring employee data to jurisdictions outside the EU, such as the US, additional considerations arise regarding data transfer mechanisms, such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs), to ensure compliance with GDPR requirements for international data transfers.

TERAMIND PRO TIP:
Teramind offers a variety of deployment options to address the customer's unique geographic footprint and international data transfer compliance setup. For more information about Teramind's deployment options, please visit:

- https://www.teramind.co/product/deployment/on-premise
- https://www.teramind.co/product/deployment/cloud
- https://www.teramind.co/deployment/aws
- https://www.teramind.co/deployment/azure

- **Legal Basis for Processing:** Under the GDPR, employers must establish a lawful basis for processing employee data, such as consent, legitimate interests, or compliance with legal obligations. When implementing UAM software, employers should identify the appropriate legal basis for monitoring activities and document their reasoning to demonstrate compliance with privacy laws.

TERAMIND PRO TIP:
We've prepared a checklist for picking the most appropriate legal basis for you here.

Legal Basis Analysis

A common perception of the GDPR is that consent is the only way to legitimize a data processing operation. This is far from the truth. Under the GDPR, a data controller has six legal bases available to them:

- Consent of the individual to the processing of their personal data (Art. 6(1)(a) GDPR)
- The processing of personal data is necessary for the performance of a contractual relationship with the individual (Art. 6(1)(b) GDPR)
- The processing of personal data is necessary for the compliance with a legal obligation to which the organization is subject to (Art. 6(1)(c) GDPR)
- The processing serves the purpose of protecting an individual's vital interests (Art. 6(1)(d) GDPR)
- The processing operation is necessary for a task that is carried out in a public interest or in the exercise of official authority vested in the organization (Art. 6(1)(e) GDPR)
- The processing of personal data is necessary for the purposes of the legitimate interests pursued by the organization (Art. 6(1)(f) GDPR).

Each of these legal bases are equal in them being a basis for a data processing operation, provided that their condition(s) are met. Sometimes, more than one legal basis applies for the same processing operation. To decide which lawful basis applies depends on the purposes and the context in which UAM software is applied. Below is an analysis of these 6 legal bases of the GDPR in the context of UAM deployment:

Consent

Requirements

Valid consent under the GDPR is (i) freely given, (ii) specific, (iii) informed, (iv) unambiguous, (v) revocable, and (vi) given with age and capacity.

- ✔ **Freely given:** Consent is freely given if the individual acts in a fully voluntarily capacity without coercion, pressure, or deception. Individuals should have a genuine choice to provide or withhold consent.
- ✔ **Specific:** Consent is specific if the individual's ascent is asked for a specific purpose (ideally, unbundled and separate from other purposes).
- ✔ **Informed:** Consent is informed if the individual receives details about the personal data processing operation to which their consent is being requested. This is where the notice comes into play. The organization's notice is designed to satisfy this component of consent.
- ✔ **Unambiguous:** Consent is clear and explicit, and expressed through a clear affirmative action such as ticking a box, clicking "I accept", or clicking an opt-in button. Silence, pre-ticked checkboxes or inactivity does not constitute valid consent.
- ✔ **Revokable:** Individuals have the right to withdraw their consent at any time. At the time consent is revoked, the data processing operation has to stop if the sole legal basis relied upon by the organization is consent. Organizations must make it easy for individuals to revoke consent. Organizations should avoid dark patterns that artificially steer individuals away from certain choices. It is important to keep records of how and when an organization has obtained consent, and what exactly the individual consented to. [4]
- ✔ **Capacity:** Additional considerations apply if the individual is a minor or lacks the legal capacity to consent.

When this legal basis is appropriate

Consent in the employment law context is a tricky issue. There is an imbalance in power in the employer-employee relationship that makes valid consent hard to come by.

Consent is only appropriate if the circumstances are such that the workers have a genuine choice and control over the monitoring taking place. A genuine choice exists if the individual can be confident that their refusal to consent doesn't carry a negative impact on their employment. This means that an employer using consent as a legal basis should do so for operations that are neutral to both parties. Examples include offering non-mandatory perks such as corporate discounts, participating in workplace birthday parties, having their photo posted on social media, and the like. This neutrality is not given for UAM software deployment. [5]

Consent is also not always required for UAM deployment. In fact, in most EU countries, there is precedent that consent is not required for work-related activities that occur at the workplace and during working time. This also applies for monitoring of company-owned devices. The employers typically rely on the legal bases of (i) legal obligation, or (ii) legitimate interest.

Under all circumstances, the company needs to:

- ✔ **Give notice:** Inform its workforce about the monitoring taking place (for more see here).
- ✔ **Conduct assessments to cover the legal basis and nature of the processing:** Prior to deploying the UAM solution, conduct a Legitimate Interest Analysis (LIA) (for more see here), Data Protection Impact Assessment (DPIA) (for more see here), or other assessments as appropriate for the nature of the UAM deployment.
- ✔ **Check for exceptions where consent is required:** Consent may be required, for example if the device being monitored by the company is company-owned, but personal use is permitted, or if employees work on their personal devices for the company (Bring Your Own Device (BYOD). Unions and works council co-determination rights may also trigger consent requirements (for more see here).

Contract

Requirements	When this legal basis is appropriate
The data processing operation is needed to fulfill the contractual obligations (or pre-contractual steps) the employer owns towards their employee.	This legal basis is only appropriate if there is no other way for the employer to comply with its contractual obligation than to deploy a UAM solution. Regulatory guidance considers these cases to be very rare. In the words of the UK Information Commissioner's Office: *"As monitoring is more often for internal business improvement purposes, it's unlikely that the contract (it) will be a suitable lawful basis for monitoring workers."* [6]

Legal Obligation

The personal data processing is necessary to comply with a law that the company is subject to. This means that the organization needs to identify the specific provision that they are subject to. A contractual obligation is not sufficient here.	A textbook case for this legal basis is the logistics company that needs to monitor, record and document the driving time, speed and distance traveled by its truck drivers and vehicles.

Vital Interests

The processing of personal data is necessary to protect an interest which is essential for the life of the data subject or that of another person.	The classic situations here involve calls to emergency services, or purposes associated with humanitarian, man-made or natural disasters. Another example is when it's important to monitor the vital signs and precise location of an employee for the purposes of their job performance, e.g. in the context of a test pilot or a rescue worker who puts himself into harm's way.

Public Authority

The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.	This legal basis covers situations such as public-private-partnerships. If the monitoring is not a necessary means to perform the public task, or if the task could be performed equally with less intrusive means, this legal basis is not appropriate.

Legitimate Interest

Requirements

The processing is (i) necessary for the legitimate interests of the organization, and (ii) the interests of the individuals do not override those legitimate business interests.

An organization relying on this legal basis has to conduct a balancing test. This balancing test is called a "Legitimate Interest Analysis" (LIA) has the following components:

- ✔ **Purpose:** The purpose of the data processing needs to be a legitimate business reason. An organization should ask questions such as:
- ✔
  - Why do we want to process this data?
  - What is the benefit we hope to gain from it?
  - How important are these benefits?
  - What is the impact if we don't go ahead with this processing?

- ✔ **Necessity:** Is the data processing solution helping to execute the purpose identified above.
  - ✓ Will this processing actually help you achieve your purpose?
  - ✓ Is the processing proportionate to that purpose?
  - ✓ Can you achieve the same purpose without the processing?
  - ✓ Can you achieve the same purpose by processing less data, or by processing the data in another more obvious or less intrusive way?

- ✔ **Individuals' rights and freedoms:** The proposed processing operation will impact the rights and freedoms of individuals. Here, the organization considers the breadth and depth of this impact, how to minimize it, and whether all things considered, the processing should prevail.
  - ✓ What are the possible impacts of the processing on people?
  - ✓ Will individuals lose any control over the use of their personal data?
  - ✓ What is the likelihood and severity of any potential impact?
  - ✓ Are some people likely to object to the processing or find it intrusive?
  - ✓ Would you be happy to explain the processing to individuals?
  - ✓ Can you adopt any safeguards to minimize the impact?

When this legal basis is appropriate

Legitimate interest is the most flexible of the six legal bases because it leaves organization room to consider their UAM configuration options and mitigation strategies to consider workers' privacy.

Key practical considerations are:

- ✔ **Documentation:** The LIA is a key piece of GDPR compliance documentation. It layers below the Data Protection Impact Assessment (DPIA) and establishes the legal basis of processing. The DPIA layers on top of the LIA, and establishes the analysis for the high risk processing operation that is involved in UAM.

- ✔ **Transparency & Notice:** See below here.

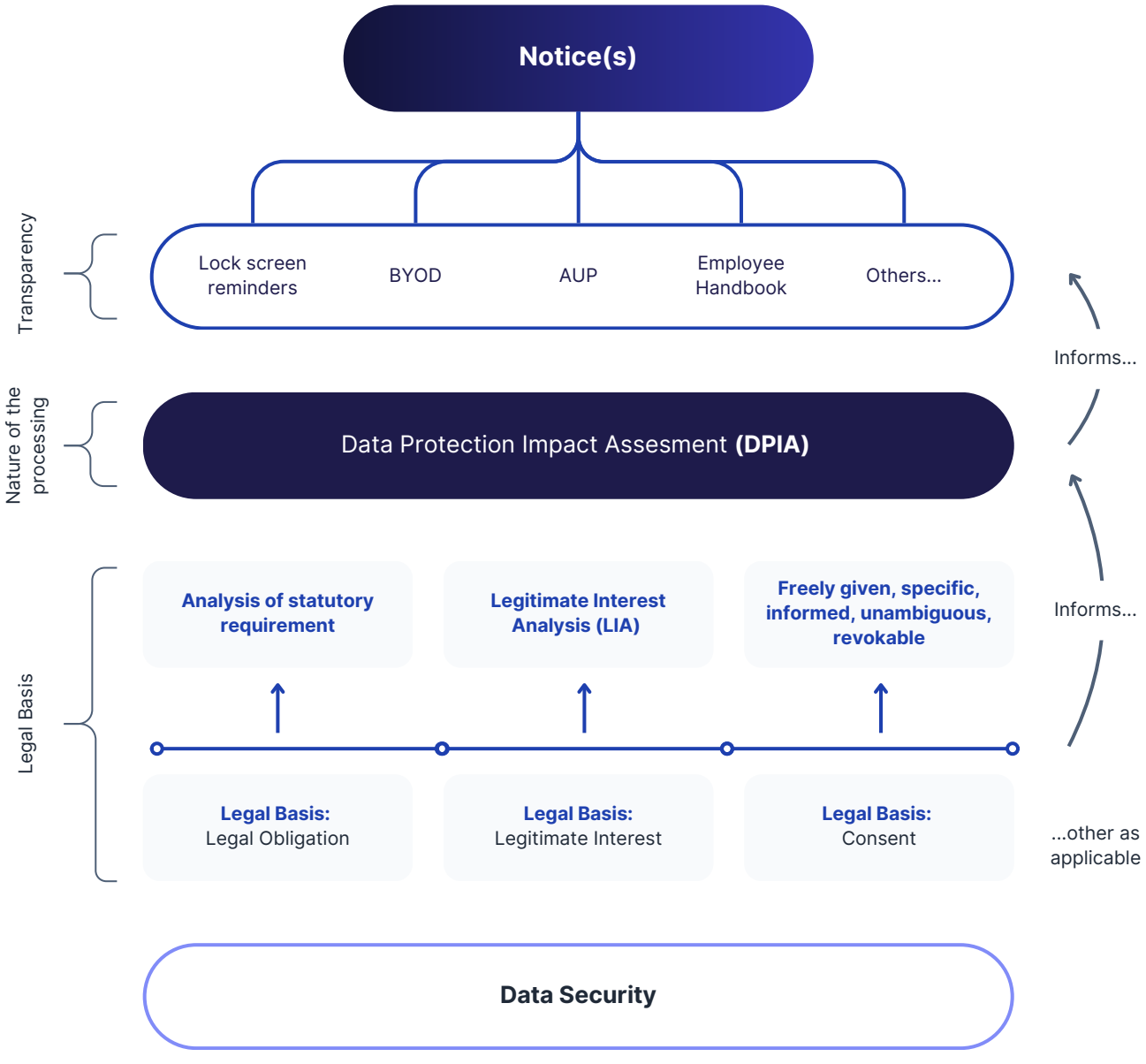
- ✔ **Data minimization:** Teramind's UAM software allows for granular controls around the nature of data points getting collected, the number of individuals and permissions to view the interface, etc.

- ✔ **Individuals' right to object & overcoming the objection:** Individuals may object to their personal data being processed on legitimate interest grounds. The balancing test conducted in the LIA, together with the DPIA, may serve to overcome such objections.

Key takeaway:

Legitimate interest-based processing provides the most flexibility for organizations where consent requirements are not triggered. For companies adopting a UAM solution, it is important to (i) clearly identify the legal basis for processing data in the UAM context (and whether this needs to be consent), (ii) be very deliberate about notice and transparency measures, (iii) conduct privacy assessments to understand the nature, scope, impact and security measures in place, and (iv) thoughtfully weave those elements together to minimize the privacy impact on the workforce.

UAM GDPR Building Blocks



Notice

Notice in the privacy law context refers to the obligation to inform individuals about an organization's data practices and policies. Notice is not, under EU privacy law, a legal basis for processing data. Notice is a disclosure of a practice. Notice typically includes the following elements:

- Purpose of the data collection
- The types of data being collected
- How (the means) of data collection
- The legal basis of the data collection
- How the data that is being collected is shared and disclosed
- For how long the data is retained
- The rights of individuals who are subject to the data collection
- The security measures attached to the personal data processing operation
- Contact details of the office where individuals may direct questions (such as the Data Protection Officer)

Notices are best provided in clear and plain language, and translated, if appropriate. Employers can deliver notice in various ways. Notice can take the shape of an Acceptable Use Policy (AUP), Bring Your Own Device Policy (BYOD), an internal privacy notice, a dedicated section in the employee handbook, or other similar means.

A best practice is for an organization to do layered notice. Layered notice means that an organization's practice is disclosed in multiple locations and with various levels of depth. For example, an organization could introduce a one-sentence disclosure on a device lock screen stating that this device is enrolled in corporate monitoring. As a next layer, the organization might add a paragraph about these practices in the employee handbook, and link out to an Acceptable Use Policy (AUP) or other resource that offers a third layer of transparency, capturing the elements of a notice listed above.

Data Protection Impact Assessment (DPIA)

A DPIA is a systematic assessment that evaluates the potential risks to individuals' privacy and data protection rights arising from a specific data processing activity prior to starting the processing operation. It involves identifying and analyzing the risks associated with data processing, assessing the necessity and proportionality of the processing, and implementing measures to mitigate or eliminate identified risks.

DPIAs are appropriate if the processing operation uses new technologies, and considering the nature, scope, context and purposes of the processing, there is a likely high risk to the rights and freedoms of individuals (Art. 35 (1)(1) GDPR). Art. 35 (4) GDPR calls out supervisory authorities to publish guidance on processing operations that they consider relevant for this provision. Regulators, including the UK ICO, have called out conducting a DPIA for deploying UAM software "a must".

In addition, DPIAs are statutorily required if:

- The processing includes automated decision-making, profiling, and where the processing is used as a basis to produce legal effects that impact an individual (Art. 35 (3)(a) GDPR)
- Sensitive data is involved (Art. 35 (3)(b) GDPR)
- A publicly accessible area is monitored at a large scale and systematically (Art. 35 (3)(c) GDPR).

The DPIA process for an in-house team looks like this:

Then: UAM software implementation

How does a DPIA tie in with the LIA?

Both LIA and DPIA involve assessing processing purpose, identifying risks, and considering safeguards. However, LIA is a lighter-weight risk assessment aimed at clarifying purpose and potential impact in the context of establishing a legal basis of processing personal data under Art. 6 GDPR. Conversely, DPIA is a thorough process with specific content and process criteria and necessary for high-risk processing, regardless of the lawful basis. Overlaps exist, so incorporating DPIA screening into LIA can help identify risks. An LIA can trigger a DPIA if it identifies high risks.

Spotlight issues

UAM Deployment Without Notice (Covert Monitoring)

Covert monitoring takes place such that the individual is unaware that their conduct on IT systems has been placed into monitoring. Under the GDPR, covert monitoring as a general business practice is hard to justify as this practice does not rely on notice and / or consent. Therefore, the transparency for individuals is lower. However, special circumstances such as gross misconduct or suspected criminal activities afoot can justify this practice. The UK Information Commissioner's Office (ICO) has provided guidance on this topic for privacy professionals where their organization leverages UAMs for these investigations [7].

Consider the following factors:

Issue	Implementation guidance
Authorizing covert monitoring	Placing an individual into covert monitoring cannot be an arbitrary decision. Senior management at the company, such as a CHRO, should be the decision-maker.
Prejudice	The company should be satisfied that there are reasonable and compelling grounds for placing an individual into covert monitoring. Further, there should be an independent assessment whether informing the individual about the monitoring would prejudice the prevention or detection of criminal activity or equivalent gross misconduct.
Data minimization	✔ Time: Set a specific time span for the covert monitoring and criteria for commencing, terminating or extending the covert monitoring. Set the monitoring timeframe to be the shortest possible, considering the investigation circumstances. ✔ Scope: Limit the systems and platforms under investigation to those that are relevant to the subject of the alleged misconduct. ✔ Minimal personnel access: Limit the number of people involved in the investigation to only those who need to be involved to achieve the purpose of the investigation. ✔ Information disclosure: Limit the number of third party recipients. Set clear guidelines who, and under which circumstances, may receive access to the personal data collected via the covert monitoring. ✔ Reasonable expectation of privacy: Covert investigation should not be deployed when the individual could reasonably expect privacy. Examples for such expectation of privacy are messages from an individual's private email address, calls to the employee's doctor, surveillance cameras in restrooms or changing rooms.
Purpose limitation	The employer may only use the information gathered through covert monitoring for the purpose intended. The employer should disregard and destroy any other information, e.g. that was auxiliary collected about third parties, unless it reveals something that no employer could reasonably be expected to ignore, and where there is no other way to achieve this purpose.
Data Protection Impact Assessment (DPIA)	A DPIA is required for personal data processing operations under the GDPR that are considered high risk for the individual. Companies deploying covert monitoring techniques will need to complete a DPIA before the investigation starts.
Data subject rights (DSR)	The individual in covert monitoring may lodge a DSR, requesting access to their personal data on file by the data controller (the employer). The company may need to disclose in part or full, depending on numerous factors such as third party data subject rights, privilege, and other considerations, the results of the investigation. A best course of action in this case is collaboration with counsel and a case-by-case analysis

Works Council Co-Determination Rights

Deploying UAMs in in certain European countries with strong employment protection laws may require the additional step of engaging with works council or social and economic committee. The French and German employment law regimes have pioneered the works council co-determination structure.

If not preempted by legislation or a collective agreement, the works council has the right of co-determination when a technical device designed to monitor the behavior or the performance of employees is being implemented. Employers engage proactively with works councils, provide transparent information, and negotiate works agreements that balance the interests of all parties involved. By fostering collaboration and addressing concerns upfront, organizations can implement UAM systems effectively while respecting employee rights and maintaining trust in the workplace.

Key issues to be aware of when engaging with German works council:

Legal Basis for UAM Deployment: Employers in Germany must establish a lawful basis for deploying UAM systems not just under the GDPR, but also under the German Federal Data Protection Act (Bundesdatenschutzgesetz). While legitimate interests or compliance with legal obligations may serve as legal bases for data processing, works council consent is often required for the implementation of UAM software as it directly affects employees' privacy rights.

Information and Consultation Obligations: Employers have obligations to inform and consult with the works council before implementing measures that significantly impact employees' interests, such as UAM systems. This includes providing detailed information about the purpose, scope, and implications of monitoring, as well as engaging in meaningful discussions with the works council to address concerns and seek their input.

Negotiation of Works Agreements [10]: In many cases, employers and works councils negotiate works agreements (Betriebsvereinbarungen) to establish rules and procedures governing the deployment and operation of UAM systems. These agreements outline aspects such as the specific purposes of monitoring, types of data collected, access rights, retention periods, and mechanisms for addressing employee concerns.

Balancing Interests: Works councils are tasked with balancing the interests of employers in maintaining productivity and security with the fundamental rights and interests of employees, including their rights to privacy and data protection. Works council consent for UAM deployment may be contingent on the implementation of safeguards to minimize intrusion into employees' privacy and ensure transparency and fairness in monitoring practices.

Challenges in Obtaining Consent: Obtaining works council consent for UAM deployment may pose challenges, particularly if there are disagreements regarding the necessity or proportionality of monitoring or concerns about its potential impact on employee morale and trust. Employers must engage in open and constructive dialogue with the works council to address these concerns and reach consensus on acceptable monitoring practices.

Companies can get a head start in these conversations by presenting works council with the privacy-preserving capabilities of the UAM solution.

1. Examples are Children's Online Privacy Protection Act (COPPA) for children's data, Health Insurance Portability and Accountability Act (HIPAA) for personal health information, and the Gramm–Leach–Bliley Act (GLBA) for consumer financial data.
2. A great resource for inhouse privacy counsel is DLA's resource available here for the US developments: https://privacymatters.dlapiper.com/state-privacy-laws/ and here for the Global landscape: https://www.dlapiperdataprotection.com/index.html.
3. The GDPR was a major push to harmonize the EU data protection landscape compared to its predecessor, the Data Protection Directive of 1995.
4. Ideally, keep screenshots of the consent flow and version control it.
5. https://iapp.org/news/a/consent-as-legal-basis-for-eu-and-u-k-employment/ and https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/monitoring-workers/data-protection-and-monitoring-workers/#dp21.
6. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/monitoring-workers/data-protection-and-monitoring-workers/#dp21.
7. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/monitoring-workers/data-protection-and-monitoring-workers/#dp19.
8. For example: Works council co-determination rights for deploying IT systems is governed by §87 Para. 1 No. 6 German Federal Works Constitution Act (*Betriebsverfassungsgesetz*).
9. The name of the works council under French law.
10. Consequences of Non-Compliance: Failure to obtain works council consent or comply with works agreements regarding UAM deployment may result in legal challenges, including claims of unlawful data processing, breach of works council rights, and violations of employee privacy rights. Non-compliance can lead to fines, legal sanctions, reputational damage, and strained labor relations.

TERAMIND

Request Your Custom Demo Now

Get Demo