

Beyond Borders: A Practical Guide to Approaching Cutting Edge Global Workplace Privacy Issues

(This transcript was generated through AI technology.)

Karla Grossenbacher: Welcome to the Workplace Privacy Podcast, where we talk about issues arising at the intersection of employment law and privacy law. Today, we're tackling a topic that can feel overwhelming even for experienced employment lawyers and HR professionals, and that's workplace privacy on a global scale. Many employers understand the rules that apply in the US, but what happens when your workforce spans Europe, Asia Pacific, Latin America, Canada, and the Middle East? The same practices that seem routine in the US can create significant compliance challenges outside the US. So to help break this down, I'm joined by my colleague, Yana Komsitsky, who advises multinational employers on international privacy issues and has tremendous experience helping organizations navigate these challenges around the world. Yana, thanks for joining me.

Yana Komsitsky: Hi, Karla.

Karla Grossenbacher: Hi. I'm so excited to have this conversation with you. Listeners, Yana and I work together all the time. Whenever there is a global flavor to a US issue that a client has brought to me, I rely on her to bring that global privacy analysis and approach and framework to those problems. So I'm excited for this discussion. Before we dive into specific workplace issues, I think many listeners would benefit from a roadmap. When employers hear global privacy, they often immediately think GDPR. But that, I assume, is only part of the picture. When a multinational employer is trying to evaluate a workplace privacy issue, what are the major regional frameworks they need to understand?

Yana Komsitsky: As far as privacy in the workplace is concerned, there are, of course, different laws in each jurisdiction, and also some trends regionally, but unlike in international labor and employment law, which I also practice and advise in, in privacy, we benefit from a lot more convergence. So in simple terms, this is because many countries look to GDPR when designing their frameworks, but often, thankfully, make compliance a bit simpler than under GDPR. We start with GDPR as the gold standard, and then relax the employer's obligations where permissible in the rest of the world.

Karla Grossenbacher: Sounds like GDPR is typically the starting point for any kind of global workplace privacy analysis. Is that right?

Yana Komsitsky: Yeah, pretty much. And then once an employer has its head wrapped around what's required for GDPR, then across APAC, LATAM, we have some flexibility and fewer obligations in many ways, although some of the concepts do thread throughout across the globe wherever there are privacy rules. And outside the US, privacy rules apply to employees just as much as they do to consumers, and really in very similar ways. So we have a lot of similarity to work with across multiple jurisdictions. There are privacy laws in nearly every location or every major location where US employers do business.

Karla Grossenbacher: If GDPR is the starting point, when an employer is faced with a new global workplace privacy question, what are the first two things—concepts—they should be thinking about as a starting point before we get into the specific use cases we're going to talk about?

Yana Komsitsky: Under laws like GDPR, there are requirements to adhere to certain principles. Under GDPR, those are lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, integrity and confidentiality, and accountability. What that means is there's really a lot more work to do before you can lawfully process employee or candidate data. Accountability is where a lot of the employer's work is. This means things like conducting data privacy impact assessments for a given use case, maintaining certain records, conducting training for any data handlers. So a lot of background work before you can actually issue a privacy notice, obtain a consent and begin processing the candidate or employee's data as intended the way you would do in the US.

Karla Grossenbacher: And that sounds like the types of obligations that the entity has, but I understand that GDPR also kind of on the flip side gives the individual employee a series of rights. And can you talk to us about what those are?

Yana Komsitsky: Yeah, there are several rights afforded to employees just like consumers in most of the world of privacy laws across the world. So where in the US the state laws really focus on consumers with the exception of the state law in California, outside the US the laws apply just to individuals in general, mostly living individuals. So of course that includes candidates and employees. Those rights are the right to know what data the employer processes in significant detail in most cases, a right to access that data to know where it goes and with whom it's shared, and that includes vendors and group entities within the employer, the right to correct that data, the right to be forgotten, subject to some reasonable limitations where the law prevents forgetting the data, the right to object to certain types of processing, where that processing is based on the employer's legitimate interests, not really where it's based on basic fundamentals of employment law, like where the employer needs to process the data to maintain the relationship. A right not to be subject to solely automated decision making or profiling, a right to withdraw consent to processing, which is a tricky one because once that's triggered, the employer has to stop the processing, even if it's embedded in a fundamental operational process. And importantly, a right to complain to the local data protection authority, which in the employment context we see often raised where there's, say, a rejection of a candidate, or it's raised as a type of sword at termination of employment or discipline or performance management whenever the relationship is starting to unravel.

Karla Grossenbacher: And if I'm understanding correctly, outside of Europe, the other regions have similar concepts and similar rights, but maybe not as stringent as what is in place or maybe as expansive as what is in place under GDPR.

Yana Komsitsky: Yes. Well, first of all, Europeans are much more aware of their rights and the protections afforded to them under GDPR than many other populations. So we

see a lot of this activity, including data subject access requests from employees, refusals to give consent. We see a lot of works council and union engagement on privacy issues in Europe, probably on the whole list. So elsewhere. But the rights do transfer to other jurisdictions. They may be a little bit more modified. And in other jurisdictions, we can think of being able to use consent a bit more liberally to process employee data.

Karla Grossenbacher: Speaking of consent, one thing that surprises, I think, many US employers and practitioners such as myself is that consent isn't always the silver bullet that we're used to it being in the US when you go outside the US. So why doesn't, as a general matter, consent solve everything internationally?

Yana Komsitsky: Yeah, so particularly in Europe, under GDPR, consent is generally disfavored as a basis for processing overall and in the employment context exceedingly so in all situations where the employee doesn't have a true binary choice or may feel pressured to agree due to the imbalance of power between employer and employee. A true binary choice is difficult in the employment context a lot of the time because that looks like—oh, I don't want to be recorded for this meeting. I don't give my consent. Does that mean I can participate in the meeting anyway? It probably means I can't, which impacts how I perform at work. And so that's not a true binary choice. So at the start of something like a meeting recording, I can't really truly consent to what's about to happen. Outside of the US, you also generally need to justify your data processing with essentially necessity, like I need to do this as an employer to maintain the employment relationship or comply with my statutory obligations under local law or another good reason. When you have another good reason, you need to balance that with the employee's privacy rights, which makes it a lot more work to do than just obtaining consent from the employee before you can actually do it lawfully.

Karla Grossenbacher: That sounds a little bit like what we think of in the US as an invasion of privacy common law balancing test. I have a legitimate reason, and then the employee has some privacy interest, but maybe not all these rights that you have under GDPR and elsewhere outside the US. So it makes, I assume, the balancing a little more complicated.

Yana Komsitsky: Yeah, and under GDPR, you're not seeking consent, whereas in other countries you are. So operationally, when you're thinking about multiple jurisdictions, you might need to modify your workflows to work in the local context. And a lot of US multinationals struggle with that because it means having to worry about 180 different processes potentially versus just one, a simple consent. We do have some interesting exceptions. In India, for instance, under the new Digital Personal Data Protection Act, it's operationally easier to deal with employee data than it is with candidate data due to some carve-outs with respect to HR activities where consent is not required. But candidates are not in an employment relationship. They're not considered to be covered by the HR activities carve out. So for those guys, you do need to obtain consent before you process their data. So again, there's sometimes a distinction in local law and practice between candidates and how you treat their data—employees—and bizarrely almost it flips sometimes. So under GDPR and in

jurisdictions that follow that type of framework, you can often get more consent from candidates than you can from employees.

Karla Grossenbacher: Interesting. So if I'm understanding the scenario, consent is typically not going to be your solution from an international perspective. But you flip to this analysis of I have a legitimate basis, reason, necessity, whatever it is, and then I have to balance that against the employee's privacy rights, essentially.

Yana Komsitsky: Yeah. And a lot of the work is in figuring out how to manage several different countries at once. So sometimes employers do lean on consent as a matter of solving for practicality, where technically there may be some questions as to whether that consent is either necessary, achieves the need that solves the problem they're trying to solve, or is technically very compliant, but at the very least, it does create an expectation in the relationship. So we do sometimes fall back on very detailed notice and then obtaining consent for certain types of data processing. But it really should be a case by case analysis for each thing that we do, even though it is strongly recommended to issue a privacy notice at the beginning of the interaction at the candidate stage and then to issue a separate privacy notice when an individual was converted to employment status, loaded into the HRIS and begins the employment relationship, because the types of processing are different. And under most laws globally, we do have to get into that level of detail explaining why we process your data differently as a candidate than we do as an employee.

Karla Grossenbacher: Well, speaking of case by case differences, let's go ahead and move from sort of the framework to handling a few different use cases in practice. A very common issue today in the US and elsewhere is recording meetings. AI note takers, transcription tools seem like they're everywhere now. And in the US, we generally analyze this under state and federal wiretapping laws and common law invasion of privacy frameworks where, as you know, consent is the cure for everything. So how does the analysis change—recording meetings, AI note takers—when you are outside the United States?

Yana Komsitsky: We definitely have it a lot easier in the US. And US employees are still more likely to give consent to that sort of thing, and we can predicate employment on it. In Europe and several other jurisdictions, this is risky, again, because consent is considered inherently coercive in the employment context. And in many other countries outside of Europe, it's also invalid and thus there's a true binary choice, which means that we have to give the employee another alternative, which is not less advantageous, whenever we're seeking their consent to processing. So with meeting note taking, that's really tough because we have to handle each individual's objection and that probably will mean not using a note taker because there is no less advantageous alternative to participate in that meeting.

Karla Grossenbacher: I understand the concept of it not being a binary choice when we're talking about, you know, an AI note taker in a team meeting where we're going to discuss a project and someone wants to have the AI note taker on so everybody knows what we discuss. How does it work if it's, say—because another common usage is

training. So we're providing this training, you are attending this training. I guess it's conceivable you could ask a question, but would it be considered a binary choice if I say, look, we're having this recording on, you can consent to it. And if you don't, you can attend the training and just sit there and not say anything. And potentially, if you have a question, you could put it in the chat if you don't want to be recorded. How would that go over?

Yana Komsitsky: That sounds more fair. There is the potential, however, that an employee will argue that they were not able to participate to the level they wanted because they felt they couldn't speak up because they didn't want to be recorded. It's a tricky area. I think offering the choice to submit via chat or perhaps afterwards is better than not offering that choice.

Karla Grossenbacher: Oh yeah, that's a good one. Come up afterwards when the recording is done and ask your question.

Yana Komsitsky: Yeah, but I think in a lot of these cases, we're operating in a gray area because the choice really isn't great. And we do see people say, you know, I don't feel like I could really engage to the same level. And I don't think I can speak freely or raise my concerns. I'm concerned in this training environment that if I say I don't understand and then that recording lives on forever, that could be used against me in performance management or it could create some bias against me. Even the fact that I don't participate or engage in a training session could result in some inferences against me and my performance at work. I think we can do it, but we have to accept that there is some risk involved.

Karla Grossenbacher: Right. And everyone has their own risk tolerances. To sum up on AI note takers recording meetings, consent isn't probably going to be your best shot unless you really have a solid alternative proposal. And then you're left with this idea of, I'm going to limit my purpose to a business process, but that carries its own problems if what I really want to do is use it for an employment purpose.

Yana Komsitsky: Yeah, and you might not think you'll use it for an employment purpose, but you might be stuck between a rock and a hard place if during the meeting someone says something that requires discipline or investigation, right? You then have what we in the US refer to sort of as fruit of the poisonous tree. We can't touch that information for investigation purposes or disciplinary purposes unless we told everybody upfront that it may be used for that. And there's certain ways to do that to cause less friction, but it does require thinking about in advance of actually needing to use it, actually, before we start using the tool.

Karla Grossenbacher: Would you be precluded from just having people who are in the meeting say, oh, yeah, I heard that comment, and disciplining on that basis, even if there is a transcript that exists—like you could say, I'm not going to rely on the transcript, I'm relying on these five people who heard you say this?

Yana Komsitsky: No, I think that would be outside of the use for which you were seeking consent. I think that consent is really more problematic in this scenario, in this use case, because really no one is really given consent.

Karla Grossenbacher: If recording creates challenges, I'm sure electronic monitoring can be even more complicated. And here I'm thinking of internet communications monitoring, badging monitoring to police an in-office work requirement or GPS tracking. And in the US, employers generally have fairly broad flexibility to monitor company systems and devices provided they address various notice requirements that are in a handful of states. How should employers think about electronic monitoring globally?

Yana Komsitsky: Yeah, it is more complicated because outside of the US, we cannot negate any expectation of privacy that they have as local residents in the way that we can in an employment handbook or privacy notice here in the US, even with California employees. So employees actually have privacy rights at work outside of the private areas like changing rooms. This includes privacy in their communications over computer systems and employer provided tools. This even includes privacy over communications for business purposes as well as personal purposes. And privacy rights in where they are physically present, so in their actual physicality where they are on the shop floor or in the office. And we see time and time again that infringing on those privacy rights without having done the heavy lifting of GDPR or other compliance could mean that the employer has compromised its ability to discipline or terminate even for bad deeds. Again, similar to what we talked about in the AI note taking use case, the evidence becomes fruit of the poisonous tree. This is one of the reasons we stress compliance in the international HR space because nearly everywhere outside the US, you need to build a case against an employee and establish cause under local law in order to terminate because there's no at-will employment.

Karla Grossenbacher: Okay, and you made a couple references to, I think, maybe video monitoring as well. So I assume the analysis is potentially the same, whether I'm electronically monitoring your communications, your badging, or I'm just trying to set up a camera and see if you're stealing from me on the shop floor.

Yana Komsitsky: Yeah, well, internet usage where the employer allows personal use is a little bit heavier regulated, but generally it is possible to monitor systems usage for nefarious activity. We shouldn't be getting into people's content, even business content without permissions. And whether that's consent or your notice depends on the jurisdiction. CCTV, however, where we're taking video footage of someone like on a shop floor is particularly heavily regulated in places like Europe and places like Quebec, Canada. There we have to justify why it's necessary, consider whether to conduct impact assessments, whether there are less intrusive alternatives, and consult with unions or seek approval from local labor authorities. And that involves a lot of specifics like mapping out where the cameras will be, what they will capture, what the postings will be on the wall near the cameras, et cetera.

Karla Grossenbacher: What would be an example of—if I want to have this camera on the shop floor to make sure you're not stealing from me, what would be a less intrusive

means? Because the only one I can think of is when you leave the shop floor, I'm going to search you, which doesn't sound less intrusive.

Yana Komsitsky: Yeah, yeah, it's a difficult one. And so for safety and security, we have good justification on a shop floor. In an office environment where there's less product to steal, we have less justification. We might talk about where we place the cameras, and we do sometimes have to negotiate with the labor inspector or the union on placement. So we don't place it at the workstation. We might place it on the product or at the door to monitor who comes in and out and with what. And we might need to rely on focusing on the product instead of the person. So that means putting things that ding when product is carried out of the store versus video watching the person all day long, which is actually under some schemes very difficult to justify.

Karla Grossenbacher: Are there signage requirements under GDPR? That's something you see in the US, you know, that people put up signs saying you're being monitored. Is that something you see outside the US?

Yana Komsitsky: Absolutely. And sometimes they can be very specific. The goal is to inform the person that is subject to the processing, in this case, the person who'll be on video, that that will happen before they enter the space where they will be on video. So all over Europe, if you're traveling as a tourist, you'll see signs that say CCTV in progress. That's quite common, expected and—again, sometimes there's a bit of negotiation required when you apply to the labor authority or work with a union on agreeing how you'll do it because they want it to be sufficiently obvious. And where it's inescapable because you need to have it for security reasons, you really need to go through the work of demonstrating that that is the case before you can just video an employee all day long because that is deemed fairly intrusive. The one thing that's even more intrusive is we're seeing a lot of AI enhanced or AI enabled video. So on things like warehouse floors or production floors on an assembly line where we're watching for health and safety purposes, using an AI enabled video to monitor whether people's movements are safe, whether they're lifting appropriately, whether they are creating spaces for walking or driving machinery, wearing hard hats, that kind of thing, that implicates biometrics rules, which add another layer of complexity, as does the situation in fleet management where we ask drivers to use video-based biometric identification or in background checking processes where we also use enhanced video or biometrics-based identification. That is a use case where we're actually using biometrics for identifying an individual and that turns the process into handling sensitive data or special category data under GDPR, which carries with it additional obligations and you actually have to justify doing that two different ways.

Karla Grossenbacher: And what are the two ways?

Yana Komsitsky: It depends on the situation, but usually you say you have something like a legitimate interest for safety or security or established legal reason, like you're required to do something as an employer and you're doing it this way. Health and safety is a very good one or security of your premises is another good one. But then because you're in special category or sensitive data territory, you probably may need to rely on

something like consent to process as well additionally, which can cause some problems because if you have a lot of drivers, hundreds or thousands, and you're asking all of them to consent, some of them may say no, and then you have to deal with that separately.

Karla Grossenbacher: Speaking of AI-enabled video, the last use case that we want to talk about is in fact AI in the form of automated decision-making technology. In the US, we don't have any federal restrictions on that. There's only a handful of states that have done anything on the topic. So what is the landscape outside the US on restricting or regulating the use of ADMTs?

Yana Komsitsky: Similar to the US, only a couple places have really given it thought. Sort of. So outside the US, there are only a few jurisdictions that have ADMT specific frameworks or AI specific frameworks. So main one being the EU where we have to consider both the GDPR rules that address this that have been in effect since 2018 and the new EU AI Act rules, including classification of certain ADMT as a high risk system under the EU AI Act. Elsewhere, we're still relying on general privacy law principles, which do govern ADMT use because ADMT is processing people's personal data. But right now, despite several countries being in process on ADMT specific legislation, it's more of a watch this space elsewhere as AI laws continue to develop. And we have some front runners like Korea, but really the EU and the US position are what's leading the compliance work at the moment as many employers, if not nearly all employers, are implementing ADMT tools. Under GDPR, European candidates and employees have a right not to be subject to a decision based solely on automated processing, including profiling, which significantly affects them.

Karla Grossenbacher: It sounds like if that's the case, you have to allow them to opt out if you're trying to use a solely automated technology since they have the right not to.

Yana Komsitsky: Yeah, the only exceptions to that right against—and that's like a fundamental principle we've had for years, right? You have a right not to be subject to solely automated processing when it really matters for a significant decision. There are exceptions in the statute and those are—it's necessary for the contract you're entering into, it's authorized by local law, which is really limited in the employment context, and we have the candidate or employee's consent. So that's quite the opposite of what we normally say about consent under GDPR, where we don't want to use it in the employment context. Here we're actually forced into it if we're going to use an ADMT type tool.

Karla Grossenbacher: So you mentioned under the EU AI Act that there is this categorization of ADMTs as high-risk systems. So if you are a high-risk system under the EU AI Act, what's the consequence? What do you have to do as an employer?

Yana Komsitsky: Yeah, so you're not always going to be in a high-risk use case as an employer, but frequently so. So anytime that you're making a decision that has significant impact on an opportunity like a hiring promotion or firing or changing the terms of employment based on an ADMT decision, you're going to be a high-risk system

use case most likely. And that means it is a case by case analysis, but most likely you will be. And that means that you have a slew of obligations to comply with. Notice of what you're doing is one, but there are many others. And they do involve collaboration with the developer of the tool to a certain extent. We see this also in California, but the definition of ADMT in California is more like the GDPR definition, not really related to the EU AI Act high risk definition, where you don't need any human involvement analysis. So you either have a high risk system or not, regardless of the level of human involvement. So that really means coordinating all your obligations across the globe when you are assessing tools to determine whether they will be California ADMT or EU AI high-risk systems.

Karla Grossenbacher: For our last topic here—and this has been such a great discussion and going through all those use cases, so fascinating to see how it plays out elsewhere—for the last topic, I wanted to ask you about global data transfers. So I think maybe sometimes companies don't think of themselves in the US as doing global data transfers, but if they have a headquarters outside the US or receive employee data from another country, maybe have a shared service center or outsourced HR support, whatever it is, what should US employers know about transferring employee data across borders?

Yana Komsitsky: Yeah, there's an inherent friction because I can't think of a single US multinational that doesn't transfer data back to the US for operational reasons. And the fundamental principle of local labor law is that you're going to be handling labor locally and really not transferring. So we have to fight for it a little bit as US employers working in a multinational environment. This is one of the areas where US employers do get caught off guard. Because in the US, we tend to think about employee data sharing as like a vendor contracting or confidentiality issue and not as the obstacle that it is internationally, particularly in GDPR countries. Outside the US, moving employee data across borders is very regulated and subject to various restrictions. There are a few countries that require some level of localization, but mostly you are allowed to transfer including share or give access to the data to individuals located elsewhere in the US or across your organization for things like emailing purposes and an employee directory and the support purposes—the administrative purposes that you mentioned, Karla.

Karla Grossenbacher: Yeah, I was just going to say I'm going to go out on a limb based on our prior discussion that we can't just seek consent to do a global data transfer.

Yana Komsitsky: We can in many jurisdictions.

Karla Grossenbacher: Oh, awesome.

Yana Komsitsky: We may need to do some other things. And this is one area where we have to do more or less a country by country analysis. So across Europe, we don't see consent, including because consent can be withdrawn, which puts us in a really awkward place once we've shared the data elsewhere, but really because we don't need to, and we do need to do some other things. So often we need to consider

whether we need to conduct a transfer impact assessment, which is analysis of where the data is going, whether there will be adequate protection once it gets there, and whether we have a transfer mechanism to protect the data to the same standard as it enjoys locally in the jurisdiction of origin. For Europe, usually that's standard contractual clauses and there's also a UK equivalent where we use those to secure or safeguard the data when it goes to countries that are not pre-approved by Europe. The US is not a country that's pre-approved by Europe. There is, generally speaking—it's not a country that's pre-approved by Europe. And then we have to remember that some data that only has local uses simply can't go even with consent. The obvious example is something like a national ID number because that has no foreseeable purpose outside of the local jurisdiction and so we shouldn't be taking it. So this isn't only coming up in Europe. Argentina, Brazil, Colombia, Mexico, Canada, China, Singapore, Korea, Malaysia, Switzerland, South Africa, Saudi Arabia, the UAE and other countries in the GCC region require some sort of adequacy determination or safety assessment, risk or impact assessment, and/or transfer safeguards such as contractual measures before we can share data or release it out of the local jurisdiction to a given country. And that is true for sharing it within our organization as well as with our vendors. And typically a US multinational will have US-based vendors that may process data in low-cost jurisdictions like India or the Philippines. And so we have to make sure that we're assessing that risk for our processing vendors as well as for ourselves as an organization.

Karla Grossenbacher: Sounds like if I'm a US employer who's going to get myself involved in transferring data outside the US, that I need to think about—what's my reason for doing this? Do I need to do this? And also, what am I going to do to meet whatever standard I need to meet to keep this data safe in the transfer and when it gets where it's going?

Yana Komsitsky: Yeah, absolutely. And we have methods for that. A lot of it involves putting in place contractual obligations on any recipient or importer of data coming from elsewhere. That gets us a lot of the way there, but you do need to know what data you need to send. And one fundamental principle of data privacy law across the globe, again, stemming from GDPR principles is data minimization. So you really have to think about whether you actually need the data on a category by category basis. So we don't want to send everything we have, we only send what we need and we only share what we need for a given purpose.

Karla Grossenbacher: All right. Well, Yana, before we wrap up, I want to give you an opportunity to leave our listeners with some parting words. So, Yana, if an HR professional or in-house lawyer remembers only one thing about analyzing global workplace privacy issues, what should it be?

Yana Komsitsky: I think it's thinking ahead before you process any data, or before you share any data. You've got to think ahead about what you need it for and what you might need it for later, and then consider what local law says about that before you do it.

Karla Grossenbacher: Brilliant. Thank you so much. Yana, this has been incredibly helpful. I think one of the most important themes from today's discussion is that global

workplace privacy isn't really about memorizing hundreds of country-specific rules, it's about learning a framework for asking the right questions. And in the US, the question is often, can you do something? But globally, the question often seems to be whether you need to do it, how do you justify it, and how do you protect the employees and their data in the process. Yana, thank you again for sharing your insights and helping us make this complex topic accessible to our listeners. It's been fantastic having you here.

Yana Komsitsky: Thank you, Karla. It's been lots of fun.

Karla Grossenbacher: And thanks to all of our listeners for joining us. We'll see you next time.