KORA Requests, Business Related Communications, and Employee's Private Electronic Devices
Public Records in Possession of Public Employees
See SB22 §10 Bill Summary Amended Statute: 45-217

KEY POINTS

- The new law does not open electronic devices owned by employees to inspection, search, data dumping, or other intrusions by employers or KORA requesters.
- Rules of discovery are not changed by this bill, only KORA provisions are amended.
- The new law applies to all "Public Records" (work related data, documents, images, etc.) made, maintained, or possessed by employees, even if not in the control or possession of the employer, regardless of whether the record is on paper or digital.
- All exceptions to open records apply to "Public Records" in the possession of an employee.
- KORA requests and determinations are handled by the employer, not the employee.

Effective July 1, 2016, Kansas law provides employment related communications on an employee's personal device is a "public record" and subject to KORA. ''Public record'' means "any recorded information, regardless of form, characteristics or location, which is made, maintained or kept by or is in the possession of: (A) Any public agency; or (B) any officer or employee of a public agency pursuant to the officer's or employee's official duties and which is related to the functions, activities, programs or operations of any public agency." '''Public record' shall not include: (A) Records which are owned by a private person or entity and are not related to functions, activities, programs or operations funded by public funds. As used in this subparagraph, ''private person'' shall not include an officer or employee of a public agency who is acting pursuant to the officer's or employee's official duties; (B) records which are made, maintained or kept by an individual who is a member of the legislature or of the governing body of any political or taxing subdivision of the state."

This change in statute has created a great deal of unwarranted consternation caused by a lack of understanding of what the new law requires. In some cases, that lack of understanding is resulting in an overreaction. People need to slow down and think about what "subject to KORA" means.

Keep in mind I am not an attorney and this is not legal advice. I am relating my understanding from the explanations given during the legislative process, the legislative documents, and a significant amount of training I have received on KORA.

My thoughts on what the new law does and does not do:

There are three significant amendments to the existing law related to this topic:

a. The definition of "Public Record" found in subsection (g)(1) adds "location" to the list of descriptors of the information under KORA rules. It also adds subsection (g)(1)(B) to the definition of "Public Record" which states information in the possession of "any officer or employee of a public agency pursuant to the officer's or employee's official duties and which is related to the functions, activities, programs or operations of any public agency" applies to KORA. This is intended to clarify the targeted information is only work related information in possession of the employee, not personal non-work related information.
b. An exemption to public records is retained from existing law without change in subsection (g)(3)(A) which states, "Records which are owned by a private person or entity and are not related to functions, activities, programs or operations funded by public funds." This provision is intended to protect private non-job related information in the employee's possession such as on a personal owned electronic device.

c. An additional exemption is added to subsection (g)(1)(A) stating, “private person shall not include an officer of employee of a public agency who is acting pursuant to the officer’s or employee’s official duty.” This is intended to draw the line between information in the possession of the employee which is personal non-work related and that generated as part of the employee’s work related functions. It further clarifies that if it is work related KORA applies and if it is not work related KORA does not apply.

Keep in mind “electronic device” or “electronic data” is not used in the law, although that was the main target of the amendment. The revised statute goes further than electronic devices and digital information. It includes ‘‘any recorded information, regardless of form, characteristics or location, which is made, maintained or kept by or is in the possession of” the employee. So it applies to paper documents an employee has in their possession as well.

The law as amended and as applied to personal owned devices only applies to business related communications. This goal was consistently spoken about during discussion and debate of the bill. It does not apply to any personal communications made on the device nor does it make any change in whether the device is subject to discovery in a criminal or civil proceeding. Discovery is an entirely different topic and discussion outside of the scope of KORA. But bottom line is nothing in this bill changes any rules of discovery.

To my knowledge, nothing in KORA or the new laws opens up a requester or an employer to do a data dump, search, look at, or anything else like that to an employee’s private phone or other electronic device. Think of how KORA requests are handled by public agencies. Those requirements and processes were not changed by this bill. As I understand it, the requests must be made to the employer. Nothing in the law states the request can go directly to the employee. When the agency receives a KORA request the requester is not allowed to come in and look through agency files. We must search for the requested items and provide them absent a KORA exception. Nothing in that has changed for the employer and it does not contain any provision expanding this as it applies to employees.

Another key point to keep in mind is that **all KORA exceptions apply to these “Public Records” in the possession of employees**. For example, criminal investigatory records are exempt; revelation of undercover officers is exempt; revelation of confidential informants is exempt; etc. There are many other existing exemptions and any of them apply to the employee’s work related communications whether in possession of the employer or the employee, including in electronic form or on an electronic device. The determination of applicability of an exception is not one the employee makes regarding “Public Records” they hold, but a decision to be made by the employer.

Comments about calls, people encountered on calls, response plans, etc. could be construed to be agency business depending on content. So everyone should be cautious about comments they make about their calls, investigations and activities in electronic format, not only on their personal device but also on employer owned devices.

I don’t see anything in KORA requiring public employees to retain records or data from their private devices. One could argue that anything the employee has that is business related could be ruled by the agency’s record retention policy, which is another discussion topic beyond the KORA changes in this bill. The statutes on records retention was not amended in this bill.

In light of this law, employers could require employees to submit business related communications to the agency at the time they are created or any time thereafter, but it doesn’t require that to be done absent a KORA request. For example, this could be accomplished by cc’ing e-mails to the

employee's business e-mail. At the least, employers certainly need a plan on how relevant KORA requests are shared with employees to see if they have any "Public Records" related to the request in their possession, including on their private electronic devices. But in the response to a KORA request, it is the duty of the employee to provide the employer with relative "public records" in their possession, including on their private electronic device. Again, this only applies to employment related data, not private communications on their device. If an employee does not give the employment related communications to their employer when requested in a KORA request both the employee and the employer could be exposed to a KORA violation. This is why prudent employers will have clear personnel rules on these new KORA provisions to protect both the employer and the employee.

A key to this is going to be in the interpretation of when information content is a "public record" versus private communications about work. Most of the time, that will probably be pretty clear.

This is not just a law enforcement issue. It affects all public employees. For that reason, we can expect local directives to more likely come from the county or city leaders than left to the law enforcement agency to establish how they will direct compliance within their jurisdiction.

Employees should remember when they communicate they are not the only ones to have that record of the communications. Anyone who receives the information, communication, or document regardless of whether it was transmitted on paper, e-mail, text message, social media, or any other means may still possess it. If that person I a public employee, what they possess is also subject to a KORA request. Remember also places like your cell phone carrier may still possess the information, but they are not subject to KORA.

Agencies should look at things like:

1. Should you have policies to require agency related communications and photos and documents on their private devices to be transferred to agency servers. For example, requiring all work related e-mail to be cc'd to their work e-mail address; photos to be transferred from their personal device to an agency server; documents they create or images of documents they capture that are work related should be transferred to the agency servers; etc. This policy should include removal of photos or evidentiary data from the device after transfer to the agency server.
2. Consider policies on text messages and how the employee provides them when they are agency business and relevant to a KORA request.
3. Consider policies on responding to or failing to respond to a KORA request, as well as intentionally concealing data subject to KORA.
4. Consider policies that clearly state that employee's personal devices are not subject to search, data dumps, or other intrusions as the result of KORA requests or issues.
5. Photos taken by officers during an investigation of any level would best reside on agency servers or in agency files and not retained by the employee electronically or otherwise. I say this not specifically related to KORA, but for the purposes of security and confidentiality as well.

Created by Ed Klumpp
ed.klumpp@KsLawEnforcementInfo.com
June 30, 2016