PARTRIDGE SNOW & HAHN LLP

THREE THINGS...

CHRISTIAN JENNER & PAUL KESSIMIAN: DIGITAL HYGIENE

DECEMBER 2019

Given the ubiquity of technology in the work place, and the staggering amount of data that we produce and process every day, every company should develop and abide by an "information governance" policy that is tailored to meet its business and legal requirements. To help in this matter, here are three things to consider doing as you go into the New Year:

1. REVIEW YOUR INFORMATION GOVERNANCE POLICY AND BE SURE IT STILL MEETS YOUR BUSINESS AND LEGAL NEEDS. Find it. Read it. If you can't get through it, then why would you think your employees could? When was it last revised? Does it still reference "floppy disks" and "zip disks"? Does it omit social media, cloud storage and mobile devices? Those might be good indications your policy needs revision. When was it last circulated to your employees? What have you done to make sure your employees understand the policy? And, by the way, is there a back room in your office that's been filled to the brim with paper records that haven't been touched in decades?

Does this seem daunting? Procrastination only makes it worse—and while you wait, the problem will simply keep expanding in terms of volume, velocity and variety. An information governance policy should consider each of these. And if that wasn't enough alliteration, there are also two other "V"s to consider: veracity and value. Said differently, how reliable is the data and is it worth the cost of managing it? Your business needs skilled information governance now, before litigation strikes and it's required to implement a "litigation hold", suspending routine document retention and destruction policies. Should this happen, non-essential digital information (as well as the warehouse-full of boxes of paper no one has touched in years) may need to be preserved, collected and reviewed—all at substantial cost to your company. The goal is to keep what you need to keep for your business and legal needs for only so long as you need to.

So, your first to-do is to review your information governance policy with pertinent stakeholders, identify data and information serving a business purpose, and agree on what your company actually needs to preserve. After you've identified what you need to keep for business purposes, the next step is to identify what you need to keep and how long based on any legal basis (*e.g.*, regulated industries often have document retention requirements imposed on them by law). As part of that process, be sure to confirm that your employees understand and agree as well, to ensure that they don't disregard or circumvent your updated information governance policy.

2. INVENTORY AND ANALYZE YOUR DOCUMENTS TO ASSURE THAT YOU ARE ACTUALLY IN COMPLIANCE WITH YOUR INFORMATION GOVERNANCE POLICY. You need to know what you have, how and why you still store and preserve it, and what belongs in the paper shredder or digital trash bin. Technology has multiplied the ways that organizations can retain materials having no further business purpose. One of the most tedious of your tasks will be to catalog the categories of electronic and paper documents in your possession, custody or control, including (a) paper and electronically stored information (ESI) currently in use *and* (b) unused hard copy records and ESI that have not yet been properly decommissioned or disposed of (*e.g.*, that closet full of filing cabinets, obsolete workstations and orphan hard drives).

Your biggest enemy is inertia: so take action now, and at every inflection point down the road. For example, when employees depart, their electronic files must be promptly organized and distributed to other employees. And don't rely solely on adding to your information governance policy a maximum retention period for certain categories of documents. Someone has to have the responsibility of flagging the date that period expires, then seeing to it that the relevant documents and data are reviewed and, absent business purpose, properly destroyed.

3. ENSURE THAT YOU CAN MEET THE LEGAL BURDEN FOR PROTECTING PRIVILEGED DOCUMENTS. As trial lawyers, we often advise businesses in responding to discovery requests, including requests for production of documents and ESI. More often than not this process includes considering and asserting legal privileges (the two most common being the attorney-client privilege and the work product doctrine) to prevent the disclosure of legal advice. It is well settled law that the party invoking privilege has the burden of establishing not only its existence but also that the privilege has not been waived. But all too often the e-discovery process will surface data and documents that *should* be privileged but, as a result of improper records maintenance, there is a risk that protection has been lost. Privilege is at risk anywhere communications made with the intention of confidential treatment were ultimately not kept confidential. Waiver could result from either *purposeful conduct* (*e.g.*, forwarding a privileged email) as well as *lack of care* (*e.g.*, saving otherwise privileged communications on an unsecured file sharing service without the appropriate safeguards). It's not enough that communications should have been kept confidential. The party seeking the benefits of privilege must establish that privilege was never waived. Your company's odds of prevailing in litigation may well depend on the quality and proper implementation of your information governance policy.

For more information on these or any related topics, feel free to contact Christian Jenner or Paul Kessimian.