April 2018

How to Generate, File, Retain and Execute Electronic HR Documents While Complying with Employee Records Laws and Electronic Signature Protocols—Worldwide

Toward a Globally-Compliant Paperless HR Operation

By Donald C. Dowling, Jr.

Littler®

Every minute of every workday, multinational employers rely on sophisticated HR information technologies to manage their global workforces. Laws worldwide regulate information technology, and so multinationals must comply, globally. Some laws regulating information technology expressly address the electronic tech context—for example, data security, data breach and data protection laws. These laws can be complex, but at least their application to electronic data processing is clear. These laws have been analyzed in detail in treaties, articles, conferences and webinars, for years. Separately, a different kind of law also regulates electronic recordkeeping, but in a way less understood in the electronic HR data context: old-school, legacy legal rules that predate the electronic era and that presuppose *hardcopy paper* documents. Our discussion here addresses how a multinational employer's electronic information systems can comply, worldwide, with old legal rules that presuppose HR documents on paper.

A multi-billion-dollar industry of tech-enabled workplace record systems has transformed the human resources profession. Employers now use cloud-based HR information systems, employee data platforms and electronic employment-records services. Today's tech-enabled workforce technology tools and cloud-based HR data platforms have rendered obsolete most old-school paper personnel files, printed employee handbooks, hard-copy HR policies and wet-ink-signed employee acknowledgements.

Multinationals' internal HR and Information Technology professionals have already migrated over to electronic—paperless—office technology. HR and IT have completely transformed how employers keep records on individual employees. Think of old-school versus tech-enabled job applications, background checking, timecards, vacation tracking, payroll, expense reimbursements, personnel files, performance evaluations, benefits enrollments (not to mention correspondence by emails and work documents on office technology platforms).

The migration from paper to electronic has revolutionized employers' broad-based communications to all employees and to subgroups—general workplace announcements, company newsletters, HR policies, benefits plan documents and everything you find on today's company intranets, as well as internal group emails. These days, employee handbooks and codes of conduct are less likely to be paper booklets than files on the company intranet.

This is all good. HR and IT teams feel no nostalgia for the era of paper personnel recordkeeping, paper HR-document archiving, paper HR communications, paper HR policies, and chasing employees down for signatures. So much paper, today, could shut down a contemporary HR department, and would make IT professionals obsolete. Imagine an office workday without email or computers—all the paper systems of a bygone era, today, would be cumbersome, even impossible to generate, archive, store and retrieve, not to mention environmentally unfriendly—*"think before you print."* Yes, modern HR information technology is vulnerable to data security threats, hacking, data breaches and data-protection-law violations. But if we converted back to mountains of paper HR records in place of today's electronic files, storing all that paper would also pose security and data-protection challenges.

But there is a legal piece here, and for multinationals, it is an *international* law issue. For multinational employers operating across borders, electronic HR recordkeeping raises significant international legal challenges that paper HR data systems do not. Again, these legal challenges fall into two categories: new laws expressly regulating electronic information technologies and old-school laws presupposing paper HR recordkeeping that do not fit the high-tech era. The first category of laws—new laws on electronic information technologies—includes laws on information security, data breaches and data protection/privacy. These electronic-data laws are complex, but they have gotten lots of attention in recent decades and are thoroughly addressed elsewhere. But the second category of laws—legacy old-school legal rules that presuppose paper documents but still regulate today's electronic records systems—have gotten less attention. This issue is poorly understood in the cross-border HR recordkeeping context of multinationals' global HR information systems.

Our discussion here addresses how to comply with laws around the world that regulate HR documents but that presuppose *paper* records. These legacy laws remain common around the world, because generally the law is slow to change. In fact, many legal rules in many countries that regulate documents, government filings and signatures—including *HR* documents, filings with government *labor* agencies, and *employee* signatures—have roots that go back centuries, but still apply today.

It is said that even now, "[d]ecades after computers took over the office environment, the paperless human resources department remains an enticing goal—but those who pursue it incautiously may come to regret their haste."[1] Multinational HR teams embracing complex and expensive electronic HR information systems face a vital legal compliance challenge: *Do multinational employers' high-tech electronic systems that generate, file, retain and execute today's HR documents worldwide comply with legacy HR document laws, around the world, that assume paper records?* Our focus here is on how a multinational employer's global HR and IT teams can set up electronic HR information platforms that generate, file, retain and execute employee records in a way that complies with document-law mandates worldwide. We focus on how a multinational can adopt worldwide, tech-enabled HR information technologies without violating old legal principles that predate technology and that assume employers print their HR documents on paper and sign them with wet ink. Our discussion breaks into three parts: (1) how to use electronic platforms to comply with HR-document-generation mandates and HR government-filing requirements worldwide; (2) how to retain and destroy electronic HR documents legally worldwide; and (3) how to collect enforceable employee electronic signatures worldwide.

Part 1: How to Use Electronic Platforms to Comply with HR-Document-Generation Mandates and HR Government-Filing Requirements Worldwide

Jurisdictions around the world impose lots of laws that require employers to generate specific types of HR documents. We might call these laws "HR-document-generation mandates." Some examples:

- *Employment contracts and statements of employment particulars*: China, Mexico and many other countries require employers issue written employment contracts. The entire European Union requires employers to give workers "one or more…*written* documents" spelling out 10 "essential aspects of the…employment relationship."[2] In the U.K., this mandatory written "statement of initial employment particulars" must spell out a list of topics including "the scale or rate of remuneration or the method of calculating remuneration," "any terms and conditions relating to hours of work (including any terms and conditions relating to normal working hours)," and "the length of notice which the employee is obliged to give and entitled to receive to terminate his contract of employment."[3]
- *Payroll documents*: Tax and employment laws in most countries have the effect of requiring employers to generate certain payroll records. Further, in England, all employees have a right to a "*written* itemised pay statement,"[4] and Brazil imposes a similar requirement. The U.A.E. requires employers of over 14 workers to maintain a written "remuneration register."[5] Costa Rica requires employers of 10 or more workers to generate a "Book of Salaries" that bears a "seal" from the Ministry of Work and Social Security Office of Salaries.[6]
- *Personnel files*: Some countries require employers to generate personnel files—the UAE, for example, requires an employer of over four workers to maintain personnel files.[7]
- *Health and safety records*: Worldwide, workplace health and safety laws require employers to generate lots of arcane workplace safety records. As one random example, Canada requires an "employer" with an "HVAC syste[m]" to "keep a record of the information required by section A-2.3.5.2 of Appendix A of the [Canadian] National Building Code and make the record readily available."[8]

1 Bloomberg BNA *Privacy & Security Law Report*, vol. 12 no. 45, "Special Report," Nov. 18, 2013 (punctuation edited).
2 EU Directive 91/533/EEC (Oct. 14, 1991), at arts. 2(1);3(1)(c) (emphasis added). The list of ten "essential aspects of the…employment relationship" appears at art. 2(2).
3 UK Employment Rights Act 1996, art. 1(4); the other requirements as to these "written statements" appear at arts. 1-7B.
4 UK Employment Rights Act 1996, art. 8(1) (emphasis added); art. 8(2) details what this "written…pay statement" must address.
5 U.A.E. Federal Law no. 8 of 1980, at art. 54.
6 Costa Rica Labor Code *as revised by* law 9343 effective July 25, 2017, art. 176.
7 U.A.E. Federal Law no. 8 of 1980, art. 53.
8 Canada Occupational Health and Safety Regulations (SOR/86-304), Div. III, art. 2.23(1).

- *Work rules and HR policies*: Laws in Costa Rica,[9] France, Japan, Korea and other countries require employers to generate written lists of work rules. Laws in Chile, Costa Rica, India, Japan and elsewhere require employers to issue written sex harassment policies.[10] U.K. law all but requires employers to issue written "disciplinary rules applicable to…employees" and "procedure[s] applicable to the taking of disciplinary decisions relating to…employee[s]."[11]

These are just a few examples of the countless laws around the world that require employers to generate specific HR documents. For our purposes, all the various HR-document-generation mandate laws in the world raise a basic electronic-HR information system question: *Can an employer comply by producing otherwise-compliant electronic—rather than paper—records? If not, can an employer electronically image a required paper record and then destroy the paper original?*[12]

Good news: Generally the answer is "yes." Usually, electronic or imaged records do comply, as long as the local HR-document-generation mandate law at issue does not specify that the required record be on paper. And that exception is rare; HR document generation mandating laws rarely say the mandatory HR document must be printed on paper. So usually an employer can plausibly take the position that the law accommodates generating and retaining only an electronic version of the required document.[13] For example, we mentioned that the U.K. requires employers to issue mandatory written "statements of initial employment particulars" spelling out a long list of topics.[14] An electronic-only version of that "statement" should comply—after all, the electronic version is *written*, just not written on paper.

Of course, any employer that will generate and retain legally-required HR documents *only* electronically should be sure each electronic document is complete and is in a format that can be printed if necessary.[15]

Still, sometimes this issue is not so clear. Sometimes a particular HR-document-generation mandate law leaves the paper-versus-electronic issue unclear. For example, we mentioned that Costa Rica requires employers to generate a "Book of Salaries" that bears a "seal" from the Ministry of Work and Social Security Office of Salaries.[16] Whether this "seal" can affix to an electronic "Book" is a question of Costa Rican administrative procedure law. This particular law presupposes paper records and may not accommodate electronic-only versions.

This example of the Costa Rica government seal requirement raises the related issue of laws that require employer *filings with government agencies*. Jurisdictions worldwide require filing certain HR documents with various government offices. Almost universally, for example, employers must file payroll records with tax and social security agencies. Many jurisdictions require submitting some workplace accident reports to government safety authorities. In the United States, an employer "order[ing] a plant closing or mass layoff" must "serv[e] *written* notice…to the State or entity designated by the State,"[17] and the EU Collective Redundancies directive imposes an even broader government-reporting obligation regarding lay-offs. European data protection authorities, particularly the one in France, require employer filings about HR data processing. Across Latin America, employers must file all sorts of HR records with various agencies. Costa Rica requires filing a copy of each worker's employment contract with the Costa Rican Ministry of Work and Social Security, Office of Employment.[18] An employer must "send" that Ministry, every January and June, a detailed headcount report.[19] Employers in Guatemala must file employment agreements with Guatemala's General Directorate of Labor within 15 days of execution. Employers in Mexico seeking binding employment releases must get the releases executed at a Mexican labor agency.

---

9 Costa Rica Labor Code as revised by law 9343 effective July 25, 2017, art. 66 et seq.
10 Chile Law No. 20,607, Aug. 8, 2012, *Diario Oficial*; Japan Equal Employment Opportunity Law of 1986 art. 11; Costa Rica law *Contra el Hostigamiento Sexual en el Empleo y la Docencia, La Gaceta*, 3 Mar. 1995, num. 45, pages 1-2.
11 UK Employment Rights Act 1996, art. 3(1)(a), (aa).
12 Obviously an employer would comply with an HR paper-document mandate if it made an electronic image of a paper record and also retained and archived the paper hardcopy. So our question here is imaging *and then destroying* the hardcopy.
13 Again, our issue here is generating and retaining these documents *only* electronically—the issue drops away if an employer makes an electronic duplicate while also archiving a paper original.
14 UK Employment Rights Act 1996, arts. 1-7B.
15 Again, our issue here is generating and retaining these documents *only* electronically—the issue drops away if an employer makes an electronic duplicate while also archiving a paper original.
16 Costa Rica Labor Code *as revised by* law 9343 effective July 25, 2017, art. 176.
17 W.A.R.N. Act, 29 U.S.C. § 2102(a)(2)(emphasis added).
18 Costa Rica Labor Code as revised by law 9343 effective July 25, 2017, art. 23.
19 *Id.* at art. 69(a).

For our purposes, all the many HR-document government-filing requirements in the world raise a basic electronic-HR question: *Can an employer comply with local government-filing mandates by generating and retaining otherwise-compliant electronic—rather than paper—HR records?*[20] Good news: The answer is always "yes"—if, that is, the agency accepts electronic filings, as is increasingly common. For example, in most countries employers and their payroll providers routinely submit electronic payroll data to government tax and social security agencies. As to those Luddite government bureaucracies around the world that still insist on paper filings, obviously employers must generate paper records (perhaps a paper print-out of an electronic document) and file paper with the agency. But the employer usually can simply turn over the hardcopy or print-out to the agency, retaining only an electronic version or image in the employer's records. The agency, not the employer, wrestles with the paper going forward.

That said, there are exceptions. Costa Rica, for example, requires employers to execute employment contracts in *triplicate*: "one for each party and one the employer delivers to the Office of Employment of the Ministry of Work and Social Security."[21] It is recommended that employers in Costa Rica and beyond retain hardcopy original wet-ink-signed employment agreements.

Part 2: How to Retain and Destroy Electronic HR Documents Legally Worldwide

In addressing how a multinational's global HR and IT teams can use paperless HR information technologies to comply with pre-technology legal doctrines worldwide, we began by addressing how laws that require employers to generate and file (with government agencies) HR documents apply to electronic records. We turn now to the next issue, retaining and destroying electronic versions of HR documents: *How can a multinational employer promulgate a legally-compliant policy or protocol on electronic HR document retention and purging?*

The United States imposes many dozens of federal, state and local HR document retention statutes that in effect command *"thou shalt retain certain HR documents for at least so long."* Accordingly, the American Society for Human Resources Management has issued a sample HR "Recordkeeping Policy" setting out a detailed schedule of specific minimum "retention periods for terminated employees' and applicants' records."[22] SHRM's HR document retention schedule dictates, for example: "[c]ompensation, job history and timekeeping records: 4 years after termination"; "FMLA and USERRA and related leave records: 3 years after termination"; [p]erformance appraisal and disciplinary action records: 4 years after termination"—and goes on to set out many other similarly-specific retention periods.

In the United States, after a statutory HR document retention period runs, the employer can usually keep the document even longer. Hanging on to an HR record beyond the "hold-by" date, in the United States, tends to be a matter of employer choice, or HR-record housekeeping and litigation strategy, not legal compliance per se. In the United States, an employer is usually free to retain or destroy no-longer-regulated HR records, as it sees fit. The employer usually can, if it wants to, retain HR documents infinitely. Even the U.S. HIPAA rule on "disposal" of "protected health information" merely requires implementing some policy addressing the "final disposition" of "protected health information"—that HIPAA rule does not affirmatively require that "protected health information" ever actually be "finally dispos[ed]."[23]

Because purging takes effort and because proactively purging records might lead to destroying information still important, many American employers tend to hang onto HR records long after they need to—although there are American employers that proactively destroy HR records after statutory retention periods run. But surely, few American employers destroy every copy of every HR record on the day after same applicable statutory retention period runs. In the United States, extra retention tends not to present compliance problems. Therefore, when American companies establish internal protocols to comply with document-retention laws, they tend to refer to the issue just as "records retention." Under law in the United States, the focus is indeed on retention, not purging.

---

20 Again, our issue here is generating and retaining these documents *only* electronically—the issue drops away if an employer makes an electronic duplicate while also archiving a paper original.

21 Costa Rica Labor Code *as revised by* law 9343 effective July 25, 2017, art. 23.

22 SHRM Recordkeeping Policy: Record Maintenance, Retention and Destruction, *available at* https://www.shrm.org/resourcesandtools/tools-and-samples/policies/pages/cms_017186.aspx.

23 45 C.F.R § 164.310(d)(2)(i). Our discussion here does not address specific HIPAA mandates as to medical records or FCRA mandates as to credit records.

By contrast, in the European Union and in Argentina, Canada, Hong Kong, Japan, Mexico, Philippines, Singapore, South Africa, South Korea, Uruguay and many countries outside the United States, omnibus data protection laws[24] impose affirmative document destruction or purging requirements. These laws make *retaining* certain records illegal. While American-style document retention laws impose minimum retain-by dates, these European-style document destruction or purging mandates are polar opposites that in theory impose maximum *destroy-by* dates. Conceptually, this is the difference between saying *"here's $1,000; I'm giving it to you on the condition that you may not spend it before next Monday"* (retention), versus saying *"here's $1,000—I'm giving it to you on the condition that you must go out and spend it all before next Monday"* (purging).

Omnibus data protection laws require proactively destroying or purging records as soon as they become obsolete. In effect, these laws tell "data controllers," including employers: *"thou shalt destroy certain HR records (after a certain point)."* Employers subject to these laws break the law if they keep a stray HR record even a day longer than necessary (albeit enforcement on this point is not rigorous). The effect is that in these countries, data protection laws force employers to spend time and resources regularly wading into their HR intranets and proactively destroying—purging—obsolete records about employees, applicants and former staffers.

But these data destruction/purging mandates tend not to impose concrete schedules or fixed destruction (purging) periods denominated in months or years. And so these laws leave employers on their own to pinpoint what day a given HR record becomes obsolete. The European Union General Data Protection Directive prohibits "stor[ing]"—retaining—personal (hence, employee, applicant and ex-employee) data after the "specified, explicit and legitimate purposes" for keeping the data fall away[25] (law in other omnibus data law countries is similar). This means employers in omnibus data protection law countries can legally retain HR documents only as long as the original "specified, explicit [or] legitimate purpos[e]" for keeping a given record remains valid. For example, under these laws, an employer is free to retain *this year's* employee attendance and expense-reimbursement records (for "specified, explicit and legitimate" payroll, attendance-policy and expense-reimbursement purposes)—but the employer must proactively go in and destroy or purge *last year's* attendance and expense-reimbursement records (assuming no "specified, explicit and legitimate purpose" remains for retaining year-old records).

One effect of these purging mandates is that any HR document an employer retains and does not purge needs a "specified, explicit and legitimate purpose." And so a strong recommendation is for employers to articulate this "purpose" for all classes of documents retained on file.

Having said that document retention mandates and document destruction/purging mandates are polar opposites, these laws almost never conflict as to any given personnel record. As to any given record, a document retention law trumps a document destruction mandate because a record still subject to a retention mandate has a "specified, explicit and legitimate" reason for being retained. Still, these two polar-opposite kinds of HR record laws raise practical compliance challenges, as one kind of law requires an employer proactively to retain certain HR documents while the other kind of law requires that same employer proactivity to go in and purge *other* HR documents.

Hence our question: *How can a multinational employer propagate a legally-compliant policy or protocol on electronic HR document retention and purging?* The answer is for the organization's HR and IT teams to collaborate on designing a global "recordkeeping policy" or protocol accounting for individual-country retention and destruction/purging requirements. It has been said that "[o]ganizations working in multiple countries will need to tailor individual records programs for each country to ensure compliance with local laws. In this case, one size does not fit all."[26] To craft a global individual records program that accounts for both document retention laws and document destruction/purging requirements internationally, factor in eight issues:

---

24 "Omnibus data protection laws" are laws that regulate all personal data, including employee data (except that Australia's omnibus data protection law excepts "employee records"). We can divide the world into two groups of countries—those that impose omnibus data protection laws (examples are listed above), and those that do not (examples include Brazil, the United States, most of Africa and the Caribbean, much of the Middle East, and arguably China).

25 GDP Regulation (EU) 2016/79 (Apr. 2016), at arts. 4(2)("processing" includes "storage"); 5(1)(b). Separately, the GDPR requires deleting certain HR data when an applicant, employee or ex-employee requests "the erasure of personal data concerning him or her." GDPR art. 17(1).

26 SHRM Toolkit, "Complying with Workplace Records and Reporting Requirements," Dec. 4, 2017, *available at* https://www.shrm.org/resourcesandtools/tools-and-samples/toolkits/pages/recordsandreportingrequirements.aspx

1. *Isolate payroll records from the policy or protocol.* Tax laws and accounting standards in almost all countries impose specific rules that require retaining tax and payroll records for fixed periods. In Spain, as one example, tax law requires retaining wage and benefits records for four years[27] and social security records five years.[28] Major employers' accounting, audit and payroll teams tend to have, already in place, solid practices for retaining payroll records in compliance with applicable tax laws and accounting standards. One reason why employers engage outside payroll providers is to preserve payroll data in compliance with local law. To craft a streamlined global HR policy or protocol on electronic HR document retention and purging, ideally the policy or protocol will isolate payroll records—carve them out, distinguish them, or address them separately. As possible, keep a global HR document retention and purging policy free of granular tax and payroll accounting provisions. The policy will define "HR records," of course. That definition, or a separate section on payroll records, could carve out *payroll* documentation, saying that the organization's internal accounting, tax or payroll protocols are separate.

2. *Inventory local (American-style) HR document retention mandates across all affected countries:* Payroll records aside, flush out every (American-style) HR document retention mandate in every country where the multinational employs staff—that is, find each local law that requires employers to retain specific categories of personnel records for some set minimum period of months or years. Fortunately, there might not be much to research here: American-style HR document retention laws can be rare outside the United States, particularly outside common law jurisdictions.

    - Spain example. In Spain, as one example, local law seems not to impose American-style HR document retention mandates. Again, payroll records are an exception, and there are some other obscure exceptions, too. But in Spain, the few exceptions are so arcane that they are "exceptions that prove the rule." Specifically, Spain's HR document retention laws (beyond payroll) are just a few obscure European Union workplace health and safety document-retention mandates, so narrow that they do not reach many or most employers. The EU requires:

        » retain work-time records of employees "performing mobile road transport activities" for two years[29]

        » "keep a list of workers exposed to group 3 and/or group 4 biological agents"[30] and keep certain other records on hazardous substances in the workplace[31] for 10 years

        » retain records on workplace exposure to carcinogens[32] and asbestos for 40 years[33]

    Someone knowledgeable will be able to research whether any (American-style) HR document retention mandates apply in any given country, quickly and cheaply. Of course, researching these laws across dozens of countries simultaneously takes longer and is more expensive. In designing a global recordkeeping policy or protocol, either include in the policy document itself an appendix that lists any applicable local-country document-retention mandates, or else have the policy require local HR and IT teams to identify those mandates.

3. *Inventory the statutes of limitations that apply to employment claims in each jurisdiction at issue.* Understand the statutes of limitations and "look-back periods"[34] in each affected jurisdiction as to administrative employment claims, harassment/bullying claims, discrimination claims, workplace injury claims, health-and-safety claims, claims involving pay, benefits and payroll—and of course dismissal claims.

    - Spain example. In Spain, for example, the statute of limitations for an employment claim is three years,[35] and for a breach-of-contract claim is 20 years.[36]

27 Spain Royal Decree 5/2000 (Aug. 2000), at art. 21(1).
28 Spain Royal Decree 84/1996 (Jan. 1996), at art. 52.
29 EU Dir. 2002/15/EC (Mar. 2002), at art. 9(b).
30 EU Dir. 90/679/EEC (Sep. 2000) at art. 11(2).
31 EU Dir. 1907/2006 (Dec. 2006) at art. 36(1).
32 EU Dir. 2004/37/EC (Apr. 2004) at art. 15(1).
33 EU Dir. 2009/148/EC (Nov. 2009), at art. 19(3).
34 A "look-back" period is the statutory period within which a court will assess damages for an ongoing violation of a timely-filed claim.
35 Spain Royal Legislative Decree 1/1995 (Mar. 1995), at art. 60.
36 Spain Civil Code (July 1889, as amended), at art. 1964.

Someone knowledgeable will be able to research HR-context statutes of limitations in any given jurisdiction, quickly and cheaply. Of course, researching these statutes across dozens of countries simultaneously takes longer and is more expensive. In designing the global recordkeeping policy or protocol, either include in the policy document itself an appendix that lists applicable statutes of limitations and lookback periods, or else have the policy require local HR and IT teams identify them.

4. *Inventory local data destruction/purging mandates across all affected countries:* Flush out every (European-style) document destruction or purging mandate in every country where the multinational employs staff. In large part this just means identifying which of a multinational's relevant countries impose omnibus data protection laws. (As mentioned, document purging mandates tend to arise under omnibus data protection laws and tend to require destroying records after they become obsolete, without imposing specific "destroy-by" timetables denominated in months or years.) Researching whether a given county imposes an omnibus data protection law is easy and cheap.

   That said, there are some European rules that require or advise employers to destroy certain records on workplace surveillance, internal investigations and whistleblower hotlines within very short "destroy-by" deadlines of just a month or so. One non-binding advisory opinion of a European Union data protection agency says: "Personal data processed by a whistleblowing [hotline] scheme should be *deleted, promptly, and usually within two months* of completion of the investigation of the facts alleged in the report."[37] Spanish law requires destroying workplace video and audio surveillance recordings within one month.[38]

   Someone knowledgeable will be able to research specific document destruction/purging mandates in any given country quickly and cheaply. In designing the global recordkeeping policy or protocol, ideally include in the policy document itself a break-out that identifies those countries that impose general destruction/purging mandates. And in the EU, the policy should address applicants, employees and ex-employees requesting "erasure" of HR data under the GDPR article 17 "right to be forgotten."

5. *Draft a provision requiring local HR in each country to retain HR documents in that country for at least set minimum periods*. Having done this research, establish in the policy or protocol itself, or perhaps as an appendix broken out by country, the minimum retention ("save until") period—denominated in months or years—for each category of HR document that the organization processes. Be sure these retention periods address the tough categories: emails, internal investigation files and records of whistleblower hotline calls. And be sure to address retention during litigation holds and under "document retention notices" in the litigation and internal-investigation context. Also, address the mechanics of retaining both paper and electronic documents.

   Each specific minimum retention period should account for the organization's own business needs and good-HR-record-housekeeping needs, but should:

   - meet any applicable (American-style) statutory retention periods (again, there may not be many of these, in many countries.
   - require retaining documents for at least the statute of limitations period for claims that might be expected to involve specific HR documents

6. *Draft a provision requiring that local HR, in each county, affirmatively destroy or purge HR documents in that country after set maximum periods.* As mentioned, minimum document retention or "save until" periods (point #5, above) are the polar opposite of destruction/purging, maximum "destroy-by," periods. Having set out retention periods (#5, above), separately the policy should also set "destroy-by" periods denominated in months or years for each category of HR documents retained. Obviously the policy's "destroy-by" date for a given document must equal or exceed the minimum retention period. Be sure these destroy-by periods address the tough categories of emails, internal investigation files and records of whistleblower hotline calls. Each "destroy-by" period should account for the organization's own business needs and good-HR-record-housekeeping needs, but should:

37 EU Article 29 Working Party Opinion 1/2006 (Feb. 2006), 00195/06/EN, WP 117, at sec. v. ¶ 2 (pg. 12) (emphasis added).
38 Spain Instruction 1/2006 (Nov. 2006), at art. 6; Spain Instruction 1/1996 (Mer. 1996) at art. 5.

- comply with any statutory destruction/purging periods (remember, statutory destruction/purging periods tend to exist mostly under omnibus data protection laws and tend not to set specific months-or-years deadlines for destruction/purging)
- fall after any applicable (American-style) statutory retention periods—again, there may not be many of these, in many countries
- make an exception for litigation holds and "document retention notices" in the litigation and internal-investigation context—but then should say when to destroy documents after litigation holds and "document retention notices" come off
- address the mechanics of destroying/purging both paper and electronic documents

7. *Articulate in the policy a clear business case for retaining documents up through the day before the policy's destruction/purging dates.* The policy document must forcefully make the case for keeping documents through the day before the policy's destroy/purge date, because if any employee or data protection authority later argues the employer retained HR data too long, beyond a destroy/purge period under local data protection law, the defense to that charge will be pointing to the policy-articulated business case for retaining documents up to the retention date, and arguing the policy itself sets out a "specified, explicit and legitimate purpose" for retaining the documents up to the destruction or purging date.

8. *Implement and enforce the policy worldwide.* Be sure local overseas management ratifies and imposes the HR document retention and destruction policy on the overseas (local) workforces. As necessary, verify that overseas local HR and IT teams fill in or supplement any local-jurisdiction-specific retention and destruction/purging periods in the policy or its appendices.

   Then, enforce the policy. Non-compliance will be dangerous: If overseas operations fail to destroy or purge records as the policy requires, then—if a challenge arises later as to premature data deletion or overlong data retention—the very existence of the policy will compromise the employer's legal position. Not issuing a document-retention and purging policy at all would be better than issuing it but then not complying.

Part 3: How to Collect Enforceable Employee Electronic Signatures Worldwide

In addressing how a multinational's global HR and IT teams can use today's HR information technologies to comply with pre-technology legal doctrines worldwide, we discussed generating/filing electronic versions of HR documents and retaining/destroying electronic versions of HR documents. We turn now to our final sub-issue: collecting enforceable employee signatures using electronic technologies rather than wet ink signatures on paper.

Employees used to have to sign lots of routine workplace papers with a wet-ink pen—background-check records-release authorizations, job applications, offer letters, payroll registrations, tax/social security forms, employment agreements/amendments, restrictive covenants, invention assignments, non-disclosure agreements, immigration documents, benefit-plan enrollments, time cards, safety logs, training attendance records, job-change and transfer notices, expatriate assignment agreements, performance reviews, benefits and equity/compensation plan enrollments (and grants), expense reimbursement forms, employee acknowledgements (of handbooks, codes of conducts, work rules, whistleblower hotlines), data privacy consents, and severance releases. These days, of course, all these records still exist. The difference is that now, onboarding new hires and existing staff can show their assent to workplace records without using a pen. According to the *New York Times*, "[t]he signature, a centuries-old way of verifying identity, is rapidly going extinct.[39] To sign onto workplace agreements, acknowledgements and forms, employees these days simply click "I agree" on online tools and intranet forms, or use an intranet portal, or send a text or email message. And these days, even where applicants and employees *do* use a pen and sign a piece of paper, the employer may image the document and destroy the paper original.[40]

39 Stacy Cowley, "Credit Card Signatures Are About to Become Extict in the U.S.," New York Times, April 8, 2018.

40 Obviously an employer would not raise electronic-signature-law issues if it made an electronic image of a paper-signed record and also retained and archived the paper hardcopy. So our question here is imaging *and then destroying* the wet-ink-signed hardcopy.

But electronic assents raise proof problems. Laws presupposing the signing of documents in wet ink are entrenched, and do not always accommodate electronic assents. It has been said that "electronic signatures are easier to forge and harder to authenticate than handwritten signatures."[41] Imagine a hypothetical boss, in any country, who just fired two employees for violating the conflicts-of-interests provision in organization's code of conduct. Imagine both employees claim they were wrongly dismissed because they had never been given the code in the first place. If these two employees' disputes end up in a local court, the employer will want to prove the employees got the code (after all, conflicts of interests are not per se illegal). Imagine Employee #1, hired first, had signed a hardcopy code of conduct acknowledgement in wet ink agreeing to abide by the code, which the employer duly filed away for safekeeping. Imagine Employee #2, hired later, must have at some point clicked "I Agree" to an electronic code of conduct acknowledgement—the organization's Information Technology department insists that all employees who onboarded since employee #2's hire date were supposed to click past a code of conduct acknowledgement screen to sign onto the company intranet system. We do not need a formal legal opinion (indeed, we do not even have to say which country this hypothetical is arising in) to understand that this employer has a far stronger case holding Employee #1 to the code of conduct acknowledgement than Employee #2.

The practical question, of course, is how to make employment-context electronic signatures enforceable: *How can an employer use its intranet and electronic HR information tools to collect enforceable employee signatures around the world without resorting to wet ink and paper archiving?* To answer this, we must draw two key distinctions: (1) wanting a memorialized employee assent versus needing a commercially-binding employee document execution; and (2) simple/permissive/minimalist employee assent law versus advanced/mandatory/digital employee execution law.

Distinction # 1: Wanting a memorialized employee assent versus needing a commercially-binding employee execution. In HR and employment law practice, professionals—HR experts and lawyers alike—often speak loosely of "employee signatures." But in employment relations, "employee signature" can mean very different things, depending on context. Broadly, we can divide the workplace scenarios where an employer asks an employee to "sign" some document into two different scenarios: situations where the employer merely wants to memorialize an employee's assent, versus situations where the employer needs a commercially-binding employee document execution.

- *Memorialized employee assent*: Usually when a request for an "employee signature" arises in the workplace, the employer merely wants some way to memorialize that the employee assents to, or requests, something. Examples:
    - » acknowledgement of an employee handbook, HR policy or code of conduct
    - » submission of a time card, vacation request or paid-time-off request
    - » sign-on to a training-attendance record
    - » submission of an expense-reimbursement request
    - » consent to a job change or transfer
    - » sign-up for a benefits program or Employee Assistance Program
    - » sign-off on a performance evaluation

In these scenarios, the employer is wise to collect proof of the employee's assent or request: If a question comes up later; the employer, prudently, has positioned itself to be able to demonstrate that, at some point in the past, the employee actually did agree to or request something. (Consider our hypothetical of the employer dismissing staff for violating a code of conduct, where the employees claim never to have gotten a copy of the code.)

41 SHRM Legal & Regulatory Report: *What Is an Electronic Signature and How Is It Used by HR Professionals?*, 6/1/2011.

- *Commercially-binding employee execution:* Under other scenarios, an employer needs an employee to execute a commercial instrument that, to become enforceable, must bear a wet-ink signature or other legally-recognized mark of execution (the document might even have to be witnessed, notarized or authenticated by a government agent). These workplace instruments are essentially worthless unless and until the employee takes some formal execution step that, under applicable law, makes the document enforceable against the employee. Examples:

    » records-release authorization to third parties (for a background check)

    » employment agreement or restrictive covenant including intellectual property assignment

    » check, loan, note, or other commercial debt instrument (employee owes or reimburses funds to the employer)

    » payroll-deduction authorization

    » payroll tax or immigration form filed with the government

    » employee equity/stock plan or award agreement

    » severance release

    With these instruments, an informal proof of assent tends not to be enough—the employee should formally execute the document in order to bring it into force.

Distinction # 2: Simple/permissive/minimalist employee assent laws versus advanced/mandatory/digital employee execution laws. Across the world, local laws impose varying standards for holding a party to a purportedly-agreed-to document. In fact, a fundamental distinction between common law (English-derived) systems as contrasted with civil law (Napoleonic code) systems is document execution. This is why notary publics often play a vital role in civil law systems but merely a formalistic role in common law systems.

Going back centuries, legal rules on document execution assumed wet-ink signatures on paper—in terms of legal history, the current era of electronic document execution is new and unsettled. That said, in recent years most countries' legal systems have played catch-up, and now feature specific legal standards for executing documents electronically. These relatively new electronic-document-execution legal standards fall into two tiers: simple/permissive/minimalist employee assent laws, and advanced/mandatory/digital employee execution laws.

- *Simple/permissive/minimalist employee assent laws:* In all legal systems these days, disputes arise over whether someone used a computer, mobile phone or other device to agree to something. Consider, for example, a dispute over whether someone really sent an email with his name at the bottom, or if he really sent a text message, or really clicked "I Agree" on some computer screen, or really submitted some computerized form on the internet, or really used a stylus or finger to e-sign a screen. In some legal systems, when one party unequivocally proves the other party really did send assent by computer, the law treats that now-proved electronic assent as binding. For example, under the California Civil Code, an "electronic signature is attributable to a person if it was the act of the person. The act of the person may be shown in any manner...."[42] When a jurisdiction holds a party to an informal computer assent like this, that law is said to be a "simple," "permissive" or "minimalist" electronic assent. In the employment context, employers generally can rely on simple/permissive/minimalist electronic assents when they need the *informal memorialized employee assents* that we discussed.

- *Advanced/mandatory/digital employee execution law:* In the centuries before the electronic age, legal doctrines evolved around executing paper documents and negotiable instruments with wet-ink signatures. In some jurisdictions in some contexts, wet-ink signatures even had to get witnessed or notarized with *someone else's* wet-ink signature. Now in the current electronic era, legal systems have tried to develop "digital fingerprints" and "encrypted digital certificates" as ways for parties to a transaction to "e-sign," substituting a high-tech digital code for a wet-ink signature. Digital signature technologies include, for example:

42 Cal. Civil Code § 1633.9(a).

» asymmetric cryptography/private computer keystrokes

» manual signature-capture devices (tablet/stylus and finger-signature pads)

» identity verification services, like affixing a unique digital code, and like email validation

» biometric signatures (fingerprints, retina scans)

An e-signed encrypted digital certificate formally recognized by law is called an "advanced," "mandatory" or "digital" signature. Examples of advanced/mandatory/digital signature legal regimes include:

» Country laws adopting the UNCITRAL Model Law on Electronic Signatures (for example, Argentina Digital Signature Law 25,506 and Switzerland Federal Law on Electronic Signatures)

» EU "eIDAS" Regulation No. 910/2014[43]

» Mexico Law of Advanced Electronic Signature 2012

» Singapore Electronic Transactions Act 2011

» South Africa Electronic Communications and Transactions Act 2002 (Act No. 25)

» The federal U.S. E-SIGN (Electronic Signatures in Global and National Commerce) Act and U.S. state laws under the U.S. Uniform Electronic Transactions Act[44]

In the employment context, ideally employers will use advanced/mandatory/digital signatures when they need the *commercially-binding employee executions* we discussed.

The best way to get enforceable employee assents is to get wet-ink signatures (ideally with a signing witness). The second-most-likely-enforceable approach is to get advanced/mandatory/digital electronic signatures that comply with the local electronic signature authorizing law. The least-likely-enforceable option is to get informal electronic assents.

In deciding whether to use electronic assents for HR documents, take three steps: First, identify which employee-executed documents around the world need a commercially-binding employee execution, which merely need a memorialized employee assent—and which do not need a signature at all. Second, develop company-wide protocols for memorializing informal employee assents—and use them consistently, around the world, for all employee electronic signatures except those that need an advanced/mandatory/digital signatures. And third, as to employee signatures that must get a commercially-binding employee execution, learn about and use locally-legal advanced/mandatory/digital signatures, or fall back on wet-ink signatures and storing paper. The rest of our discussion addresses these three steps.

1. *Identify which employee-executed documents around the world need a commercially-binding employee execution, which merely need a memorialized employee assent—and which do not need a signature at all.* We discussed that many of an employer's purported needs for employee "electronic signatures" really just call for a simple memorialized employee assent, rather than a formal commercial document execution. Distinguish which workplace "electronic signature" scenarios are which. We mentioned that simple memorialized employee assents are usually appropriate for code-of-conduct acknowledgements, training attendance logs, shift-change notices, expense reimbursement requests, paid-time-off requests, performance evaluations and the like, but there are overtly contractual workplace HR documents that need to get executed formally—for example, employment agreements, invention assignments, equity plan awards, restrictive covenants and severance releases. For those, advanced/mandatory/digital signatures, or wet-ink paper signatures, offer the employer the best proof.

43 July 2014.
44 E.g., South Carolina Code Ann. §§ 26-6-10 to 26-6-210.

Distinguishing which HR documents need which type of execution can mean the difference between winning and losing a dispute. For example, in 2014 the Ontario Superior Court of Justice refused to enforce a would-be employment contract purportedly "executed" by a simple email[45]—the result would have been different if the parties had used a demonstrable advanced/mandatory/digital signatures (or wet-ink) signature. Similarly, in a 2014 California case, the employer lost because it had had its employee put a simple memorialized employee assent on an arbitration agreement.[46] That result, too, would have differed if the employer had used a demonstrable advanced/mandatory/digital (or wet-ink) signature. In a different 2014 California case, a court upheld without question an employment agreement that an employer and employee had electronically executed using DocuSign.[47]

In distinguishing which workplace "electronic signature" scenarios are which, remember that outside the United States more documents will need formal, commercially-binding executions. Take onboarding. Under U.S. employment-at-will, employees tend not to enter into written employment contracts, and even "offer letters" do not always bear an employee signature. But law in other jurisdictions affirmatively requires employees execute formal employment contracts. There are written-employment-contract-mandating laws like this, for examples, across the entire European Union (although the EU allows substituting not-executed statements of employment particulars[48]) plus in Albania, Bahrain, Chile, China,[49] Costa Rica,[50] Egypt, Ghana, Guatemala, Indonesia, Kenya, Korea, Kosovo, Mexico,[51] Nicaragua, Nigeria, Oman, Qatar,[52] Russia, Tanzania, Uganda, and Vietnam.

2. *Develop company-wide protocols for memorializing informal employee assents—and use them consistently, around the world, for all employee electronic signatures except those that need an advanced/mandatory/digital signature.* Working with the IT department, design an internal system for collecting memorialized employee assents (simple/permissive/minimalist employee assents) around the world. The system needs to enable the employer to prove employees actually assented, even years before.

   Road-test the system by playing out scenarios contesting employee assents. What if the employer might someday have to prove that some employee in a far-flung office had, years before, clicked "I Agree" to the code of conduct acknowledgement (if that employee later claims never to have seen the code)? Will the IT team be able to produce actual proof admissible in a local labor court of that employee's assent?[53] Consider, for example, an internal expense-reimbursement system. What if one day a boss catches an employee cheating on an expense reimbursement, but the employee denies having affirmed the fraudulent expense submission and claims it was a mere draft, or was submitted accidentally, or blames his secretary? Will the IT system have the functionality to prove the employee formally submitted that particular reimbursement request?

   In designing internal employee assent protocols, be prepared to make trade-offs and to tolerate some risk. Informal workplace electronic employee assents happen constantly every workday, but only a tiny fraction later get challenged and litigated in court.

   The "acid test" of any informal employee electronic assent is whether the assent would be admissible, persuasive evidence in a local court. An electronic workplace assent that local courts will not enforce is worthless as soon as some employee denies or challenges it. That said, understanding and accounting for every local court's evidence rules is a huge exercise.

---

45 *Free v. Municipality of Magnetawan* , 2014 ONSC 3635 (Sept. 8, 2014)(in this case it was the would-be employee who tried to hold the would-be employer to the alleged email employment contract).

46 *Ruiz v. Moss Bros. Auto Group*, 232 Cal. App. 4th 836 (Cal. Ct. App. 4th Dist. Div. 2, 2014)(later proceeding, unpublished opinion of Mar. 10, 2017).

47 *Woods v. Victor Marketing Co.*, U.S. N.D. Cal., case no. C-14-0264 (interim order of 8/28/14), *available at* https://docs.justia.com/cases/federal/district-courts/california/candce/3:2014cv00264/273671/54.

48 EU Directive 91/533/EEC.

49 China Employment Contract Law of 2008, art. 10.

50 Costa Rica Labor Code as revised by law 9343 effective July 25, 2017, art. 23.

51 Mexico Labor Code, art. 24.

52 Qatar Labor Law No. 14 of 2002, art. 38.

53 For example, *Ruiz v. Moss Bros. Auto Group*, supra, 232 Cal. App. 4th 836 (Cal. Ct. App. 4th Dist. Div. 2, 2014)(later proceeding unpublished opinion of Mar. 10, 2017) is an example of a case in which an employer's IT team could not meet the burden to prove the existence of an employee electronic assent.

3. *As to employee signatures that must get a commercially-binding employee execution, learn about and use locally-legal advanced/mandatory/digital signatures, or fall back on wet-ink signatures and storing paper.* We mentioned the California case where an employer could not meet its burden to prove a simple/permissive/minimalist electronic assent on an arbitration agreement.[54] The employer lost that case because it did not have a demonstrable advanced/mandatory/digital electronic signature. The lesson is that in those situations that call for a demonstrable execution of a commercial-type instrument, either get an advanced/mandatory/digital signature or fall back to a wet-ink signature.

   As a practical matter, a wet-ink-signed paper document usually amounts to the best proof of all. But in theory, jurisdictions that recognize advanced/mandatory/digital electronic signatures should enforce them like wet-ink signatures on HR documents, just as those jurisdictions would enforce compliant formal electronic signatures in the commercial and negotiable instrument contexts. Remember that, to be enforceable, an advanced/mandatory/digital signature must meet local legal requirements for document execution. When using a commercial platform like DocuSign, the question is whether the DocuSign functionality meets the local jurisdiction's particular advanced/mandatory/digital electronic signature requirements.

   In some cases an employer might collect wet-ink signatures, but then electronically image them and destroy the originals.[55] When a dispute over a signed document may be headed to court but only a pdf image of the document exists, the best the employer will be able to do is print up the imaged document and produce the print-up. As with electronic assents, the "acid test" of enforceability is the question of admissibility in court and weight of the evidence. This issue will be fairly straightforward in the United States and certain other common law jurisdictions where the so-called "best evidence rule" should admit a printed pdf, if the original was destroyed and the pdf is the best extant evidence. But under the "best evidence rule" (also called the "original writing rule"), where a document was executed in counterparts and the employee's original is available, the employee's version likely controls, absent evidence of tampering or forgery. In any event, the "best evidence rule" is a common law doctrine. Civil law countries more rigorously emphasize document formalities; expect them to be significantly stricter, often requiring original hard copies. Expect civil law courts to hold employers to their burden to authenticate documents claimed to have been duly executed. In these countries, employees are less likely to stipulate to or concede document authenticity.

Conclusion

Electronic information technologies have revolutionized human resources. No multinational employer is looking back and longing for the days of paper personnel recordkeeping and wet-ink employee signatures. But around the world, electronic HR recordkeeping raises significant international legal challenges that fall into two categories. The first category is new laws designed to regulate electronic information systems—information security law, data breach notification mandates and data protection/privacy regimes. These new technology laws have been extensively analyzed in recent years in treatises, articles and seminars. The second category of laws that reach electronic HR records, though, is more obscure: Old-school laws that predate and therefore presuppose *paper* HR recordkeeping but that need interpretation in the context of today's electronic HR information systems and technologies. Fortunately, these laws can work even today, in the information age. A proactive multinational can indeed implement viable electronic systems, worldwide, for complying with: (1) "HR-document-generation mandates" and HR government-filing requirements; (2) requirements to retain and destroy HR documents; and (3) employee signature protocols. But a multinational employer needs to design a viable cross-border compliance strategy.

54 *Ruiz v. Moss Bros. Auto Group*, 232 Cal. App. 4th 836 (Cal. Ct. App. 4th Dist. Div. 2, 2014)(later proceeding unpublished opinion of Mar. 10, 2017).

55 Obviously an employer that images a wet-ink-signed agreement but retains the paper copy does not raise any electronic-signature-law issue. So our question here is imaging *and then destroying* the hard-copy.


Littler
Employment & Labor Law Solutions Worldwide®