EXCERPT

THE LITTLER NATIONAL EMPLOYER LIBRARY

LITTLER ON DATA PROTECTION & RELEASE OF PERSONAL INFORMATION:

HIPAA & Related Laws

Authors:
Philip L. Gordon
Kwabena A. Appenteng
Morgan J. Matson

Littler | EMPLOYER LIBRARY

ABOUT THE AUTHORS

Philip L. Gordon is a shareholder in the Denver office of Littler Mendelson, P.C., the largest U.S.-based law firm exclusively devoted to representing management in labor and employment law. He is also co-chair of the Privacy and Background Checks Practice Group. Philip has years of experience litigating privacy-based claims and counseling clients on all aspects of workplace privacy and information security. He has provided advice to businesses of all sizes on: surveillance of employees' electronic communications; the Federal Wiretap Act; the Federal Stored Communications Act; workplace searches; location tracking and use of GPS-enabled devices; background checks, the Fair Credit Reporting Act (FCRA); social media and other new technologies affecting the workplace; the Health Insurance Portability and Accountability Act (HIPAA); state data protection laws; responding to security breaches; the European Union Data Protection Directive; global data protection laws; cross-border transfers of human resources data; outsourcing; and the Genetic Information Nondiscrimination Act (GINA). Philip also has substantial experience representing employers in disputes involving misappropriation of trade secrets, claims of unfair competition and charges of wrongful termination. In addition, he regularly counsels businesses on compliance with the Americans with Disabilities Act's Accessibility Guidelines and frequently defends businesses against claims of public accommodation discrimination. Philip writes extensively on workplace privacy issues and has given dozens of presentations on the topic.

Kwabena A. Appenteng is an associate in Littler's Chicago office. He represents and counsels clients on a range of employment issues with a focus on workplace privacy issues, including responding to security breaches, state data protection laws, social media laws, workplace surveillance laws and issues stemming from the Health Insurance Portability and Accountability Act (HIPAA). Kwabena is a Certified Information Privacy Professional for the U.S. private sector and Europe (CIPP/US; CIPP/E). These credentials from the International Association of Privacy Professionals (IAPP) indicate his understanding of global concepts of privacy and data protection laws, and how these components apply in the workplace. Kwabena is a frequent writer on privacy topics, and has been published in a variety of publications. He also routinely speaks and gives presentations on privacy-related topics.

Morgan J. Matson, an associate in Littler's Pittsburgh office, provides strategic advice and counsel to multinational employers on a wide range of employment and compliance matters. Morgan regularly advises employers on the intricacies associated with managing a global workforce, including such areas as data privacy, global codes of conduct and international policies and global mobility and expatriate programs. She frequently publishes and speaks on data privacy issues.

COVERAGE

Scope of Discussion. The unauthorized access to and improper disclosure of personal information has serious consequences to both organizations and the individuals involved. There are several federal and state laws that: govern the myriad types of personal information (Social Security numbers, health information, etc.); define *personal information*; determine whether, and to what extent, employees can access their own personnel files; govern the use, disclosure, and destruction of various types of personal and health information; and dictate notification requirements when there is a data breach. This publication also looks at international laws in this area, including the European Union's strict data protection laws. The publication is designed to provide an employer with an overview of potential areas of risk and offers compliance guidance on several topics.

Although the major recent developments in federal employment and labor law are generally covered, this publication is not all-inclusive and the current status of any decision or principle of law should be verified by counsel. The focus of this publication is federal law. Although some state law distinctions may be included, the coverage is not comprehensive.

To adhere to publication deadlines, developments and decisions subsequent to **January 9, 2017** are generally not covered.

Disclaimer. This publication is not a do-it-yourself guide to resolving employment disputes or handling employment litigation. Nonetheless, employers may find the information useful in understanding the issues raised and their legal context. This publication is not a substitute for experienced legal counsel and does not provide legal advice regarding any particular situation or employer or attempt to address the numerous factual issues that inevitably arise in any employment-related dispute. The materials in this publication are for informational purposes only, not for the purpose of establishing an attorney-client relationship. Use of and access to this publication does not create an attorney-client relationship between Littler Mendelson, P.C. and the user.

§ 2 CONFIDENTIALITY OF OTHER PERSONNEL/EMPLOYEE RECORDS

§ 2.2 LIABILITY FOR UNAUTHORIZED ACCESS TO & IMPROPER RELEASE OF PERSONAL INFORMATION

§ 2.2(a) *Data Breaches Leave Employers at Risk*

Wherever protected data is collected and processed, the risk of a data breach exists. When a breach occurs, the central questions are: (1) Who must be notified? and (2) When? An amalgamation of laws in 47 U.S. states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands protects consumers, employees and others by mandating that citizens be notified when the security of their personal information has been compromised.[1] The rationale underlying compulsory breach notification laws is that a business forced to inform its consumers or employees that their personal data has been compromised will improve information security measures to avoid having to provide such a notification in the future.

Security breaches have serious consequences to both the organizations and the individuals involved. Figures provided by the Privacy Rights Clearinghouse, which tracks security breaches in publicly available sources, demonstrate the prevalence of data breaches:

Table 1. Data Breaches - Private Records Improperly Disclosed/Accessed by Unauthorized Personnel[2]	
Year	**No. of Records**
2012	over 27.9 million
2013	over 60.9 million
2014	over 67.9 million
2015	over 160.0 million
2016	over 11.0 million

The entities involved in such breaches include financial and insurance services companies, retailers, educational institutions, government and military, health care providers and nonprofit organizations. The reported causes of these security breaches were manifold, including: dishonest insiders; lost or stolen laptops, computers or backup tapes; and hacking.[3]

Additionally, data/security breaches continue to be costly in terms of out-of-pocket costs and loss of business reputation for businesses:

[1] *See, e.g.*, ARIZ. REV. STAT. § 44-7501; CAL. CIV. CODE §§ 56.06, 1785.11.2, 1798.29, 1798.82; LA. REV. STAT. §§ 51:3071 *et seq.*; N.C. GEN. STAT § 75-65; VT. STAT. ANN. tit. 9, §§ 2430 *et seq*. For a complete list of states and applicable statutes, see http://www.ncsl.org/default.aspx?tabid=13489.

[2] Information from the Privacy Rights Clearinghouse can be found at https://www.privacyrights.org/data-breach.

[3] Privacy Rights Clearinghouse, Chronology of Data Breaches, *available at* http://www.privacyrights. org/data-breach.

Table 2. Data Breaches - Cost to Organizations[4]			
Year	**Average Cost per Lost or Stolen Record**	**Average Total Cost of Data Breach**	**Average Lost Business Costs**
2012	$194/record	$5.5 million	$3.0 million
2013	$188/record	$5.4 million	$3.0 million
2014	$201/record	$5.9 million	$3.3 million
2015	$217/record	$6.5 million	$3.7 million

There is also the risk of class-action litigation arising out of a security breach involving the loss or theft of personal information. Notably, there is a growing number of cases allowing individuals whose identity is actually compromised as a result of a data breach to sue the companies responsible. The Eleventh Circuit Court of Appeals in *Resnick v. AvMed* held that plaintiffs claiming actual identity theft resulting from a data breach had standing to sue the company that suffered the compromise.[5] The Eleventh Circuit reversed the dismissal of plaintiffs' negligence, breach of contract, breach of fiduciary duty and unjust enrichment claims.[6] In *Resnick*, two laptops containing sensitive customer information were stolen from the corporation's office. Ten and 14 months after the theft, two customers whose information was on the stolen computers allegedly became the victims of identity theft and suffered monetary losses. The court held that the plaintiffs had standing to sue because they suffered an injury that was fairly traceable to the corporation's alleged failure to secure the data on the laptops.[7] The plaintiffs also sufficiently pled causation of damages for all of their claims because there was a nexus between the data breach and the identity theft that relied on more than just coincidence in time and sequence of events.[8] Thus, securing sensitive information of customers and employees, as well as corporate technology and mobile devices, is more important than ever.

The Seventh Circuit Court of Appeals has gone further by ruling that plaintiffs have standing to sue simply for the time and expense of preventing fraud on their accounts by taking such preventive measures as monitoring their credit score and securing replacement cards.[9]

Thus, it is critical that employers take steps to safeguard not only the information it has about its own employees, but any personal information it may have about clients, customers, etc.

§ 2.2(b) *Identity Theft in the Workplace*

The U.S. Federal Trade Commission (FTC) issued a guide to businesses in 2013 for complying with the FTC's 2007 *red flags rule*, which "requires many businesses and organizations to implement a written identity theft prevention program designed to detect the 'red flags' of identity theft in their day-to-day operations, take steps to prevent the crime and mitigate its damage." The 14-page guide, "Fighting Identity Theft with the Red Flags Rule: A How-To Guide for Business," includes a description of which businesses must comply with the rule, frequently asked questions and a four-step process for complying

---

[4] Ponemon Institute, *2015 Cost of Data Breach Study* (May 2015), *available at* https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03055USEN&attachment=SEW03055USEN.PDF.

[5] 693 F.3d 1317 (11th Cir. 2012).

[6] 693 F.3d at 1321.

[7] 693 F.3d at 1323–24.

[8] 693 F.3d at 1327–28.

[9] *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963 (7th Cir. 2016); *Remijas v. The Neiman Marcus Grp. L.L.C.*, 794 F.3d 688 (7th Cir. 2015).

with the rule's requirements.[10] As a result of this guidance, businesses should determine whether they are required to have a written identity theft prevention program.

§ 2.2(c) *Federal & State Developments*

Federal Developments

For private sector employers, the FTC has been particularly active in filing enforcement actions against companies that suffer data breaches, including cyber-attacks. In 2015, the Third Circuit Court of Appeals issued its decision in *Federal Trade Commission v. Wyndham Worldwide Corp.*[11] After the company suffered three cybersecurity attacks between 2008 and 2009, the FTC filed suit, alleging the company engaged in unfair cybersecurity practices that "taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft."[12] In affirming the district court's decision to deny the company's motion to dismiss, the Third Circuit rejected the company's argument that it did not engage in an unfair practice because it was victimized by criminals and held that a cybersecurity attack could still be deemed to be an unfair practice if the harm suffered was foreseeable. The Third Circuit's ruling provides private sector employers with an additional reason to ensure that they are taking appropriate measures to protect against data breaches. The Eleventh Circuit Court of Appeal's 2016 decision in *LabMD, Inc. v. Federal Trade Commission*, however, made clear that the FTC's ability to bring an enforcement action against a company that suffers a data breach is limited to cases in which consumers have suffered an actual harm, and not a mere intangible harm.[13]

In 2015, the FTC issued a guide for companies, *Start with Security*, on ensuring that consumer data is securely stored and disposed.[14] In 2016, the FTC issued a second guide, *Data Breach Response*, which provides businesses with tips on the steps to take once a data breach has occurred.[15] Also in 2016, the FTC issued guidance explaining the Commission's view on compliance with the Department of Commerce's National Institute of Standards and Technology's (NIST) Cybersecurity Framework.[16] According to the FTC, while the framework was intended to provide organizations with a compilation of industry-leading cybersecurity practices that organizations should consider in building their cybersecurity programs, applying the framework is also one way for a company to ensure it has implemented reasonable data security processes.

Finally, on January 9, 2017, as this title went to publication, lawmakers reintroduced the Email Privacy Act (H.R. 387), a bill intended to amend the Electronic Communications Privacy Act of 1986 (ECPA). The bill is designed to update the privacy protections for electronic communications information that is stored by third-party service providers by prohibiting the government from obtaining e-mail communications from a provider of an electronic communication service (such as an employer's e-mail network) without a warrant, regardless of how long the communication has been held in electronic

---

[10] *See* http://www.business.ftc.gov/documents/bus23-fighting-identity-theft-red-flags-rule-how-guide-business.

[11] 799 F.3d 236 (3d Cir. 2015).

[12] 799 F.3d at 240.

[13] Case No. 16-16270 (11th Cir. Nov. 10, 2016).

[14] U.S. Federal Trade Comm'n, *Start with Security: A Guide for Business* (June 2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[15] U.S. Federal Trade Comm'n, *Data Breach Response: A Guide for Business* (Oct. 2016), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0154_data-breach-response-guide-for-business.pdf.

[16] U.S. Federal Trade Comm'n, *The NIST Cybersecurity Framework and the FTC* (Aug. 2016), *available at* https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc.

storage. Currently under the ECPA, the government does not need to obtain a warrant for e-mails that have been stored for longer than 180 days.[17]

State Developments

At the state level, the growing threat of identity theft has prompted virtually every state to enact laws limiting the use and disclosure of personal information. These laws generally fall into four categories:

1. laws that restrict the use of Social Security numbers;

2. laws that regulate the destruction of certain types of personal information;

3. laws that require businesses to notify individuals whose personal information, maintained by the business, has been compromised through acquisition by an unauthorized person; and

4. laws that require business to implement safeguards for personal information, including detailed requirements in some states, such as Massachusetts[18] and Oregon.

§ 2.2(c)(i) *Laws Restricting Use of Social Security Numbers*

Social Security numbers are of special interest to persons who commit identity theft because they are a broadly used unique identifier and, therefore, particularly useful in perpetrating such fraud. As a result, several states have enacted legislation aimed at protecting the privacy and security of Social Security numbers. These statutes generally prohibit businesses, including employers, from:

- posting or publicly displaying an individual's Social Security number;

- using such numbers on identification cards;

- requiring the transmittal of employee Social Security numbers over the Internet, except via a secure (*i.e.*, encrypted) connection; and

- mailing any document containing a Social Security number (unless the Social Security number is required by law to be placed on the document).[19]

An increasing number of states, such as California, New York and Texas, broadly require businesses that collect Social Security numbers and other sensitive personal information, such as driver's license numbers, to implement reasonable safeguards for that information.[20] Massachusetts and Oregon go a step further and require such businesses to implement comprehensive security programs and provide detailed

---

[17] 18 U.S.C. § 2703(a).

[18] Notably, Massachusetts now has an online data breach notification archive that tracks the number of data breach notifications received by the Massachusetts Office of Consumer Affairs and Business Regulation since the Commonwealth's notification law took effect. *See* http://www.mass.gov/ocabr/data-privacy-and-security/data/data-breach-notification-archive.html.

[19] Idaho and Maine have taken very limited approaches to their respective restrictive use statutes. Idaho only prohibits a person from intentionally communicating an individual's Social Security number. IDAHO CODE ANN. 28-52-108. Maine only prohibits persons from using a Social Security number on a credit card, customer service card or debit card. ME. REV. STAT. ANN. tit. 10, § 1272.

[20] CAL. CIV. CODE § 1798.85; CAL. LAB. CODE § 226; N.Y. GEN. BUS. LAW § 399-ddd; TEX. BUS. & COM. CODE §§ 501.001 *et seq.*

requirements for such programs.[21] Finally, a small minority of jurisdictions, such as Connecticut and Michigan, require that employers implement and post a privacy policy that addresses their use of Social Security numbers.[22]

The federal judiciary also requires attorneys to redact certain personal identifying information of individuals involved in litigation when filing documents in federal court—either electronically or in traditional paper format. Rule 5.2(a) of the Federal Rules of Civil Procedure reads:

> Unless the court orders otherwise, in an electronic or paper filing with the court that contains an individual's social-security number, taxpayer-identification number, or birth date, the name of an individual known to be a minor, or a financial-account number, a party or nonparty making the filing may include only:
>
> (1) the last four digits of the social-security number and taxpayer identification number;
>
> (2) the year of the individual's birth;
>
> (3) the minor's initials; and
>
> (4) last four digits of the financial-account number.

§ 2.2(c)(ii) *Laws Regulating Destruction of Certain Types of Personal Information*

More than half of the states have enacted legislation requiring businesses to take reasonable steps when destroying records that contain personal information to ensure that the personal information cannot be retrieved by, for example, "dumpster divers."[23] Although the laws in some of these jurisdictions apply only to customer records, employers should, nonetheless, consider developing policies and practices for properly destroying records containing personal information of employees because these records also can be used to commit identity theft.

For purposes of the document destruction statutes, *personal information* generally means an individual's name accompanied by other information such as the individual's Social Security number, credit or debit card number, savings or checking account number or driver's license number. Reasonable measures to destroy records include:

1. burning, pulverizing, recycling or shredding of papers containing personal information so that the information cannot practicably be read or reconstructed; and

2. the destruction or erasure of electronic media and other nonpaper media containing personal information so that the information cannot be retrieved.

A business may hire a third party to help destroy personal information in a manner consistent with the document destruction statutes so long as the business takes steps to ensure the competence and reliability of the party hired for this purpose.

---

[21] 201 MASS. CODE REGS. §§ 17.01–17.04; OR. REV. STAT. §§ 646A.600 *et seq.*

[22] CONN. GEN. STAT. § 42-470; MICH. COMP. LAWS §§ 445.81 *et seq.*

[23] *See, e.g.*, ARIZ. REV. STAT. § 44-7601; CAL. CIV. CODE § 1798.81; COLO. REV. STAT. § 6-1-713; FLA. STAT. § 501.171(8); 20 ILL. COMP. STAT. 450/20; N.Y. GEN. BUS. LAW § 399-h (excluding only individuals who do not conduct business for profit).

Relatedly, as part of its efforts to combat identity theft, the FTC promulgated regulations requiring the proper destruction of *consumer information*. *Consumer information* is defined to include credit reports, or information derived from such reports, used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for employment.[24] The federal regulations do not mandate any specific methods or equipment for disposing of such information, but instead require businesses to take "reasonable measures" to safeguard consumer credit information.[25]

Under the regulations, *reasonableness* may be determined by considering: (1) the sensitivity of the consumer information; (2) the nature and size of the business's operations; (3) the costs and benefits of different disposal methods; and (4) relevant technological changes.

The regulations list as illustrative examples:

- burning, pulverizing or shredding of paper documentation;
- destruction or erasure of electronic media; and
- contracting with a third party that engages in the business of destroying such information, so long as such contract is entered into after due diligence, and the third party's compliance with this rule is monitored and audited by the contracting business.

§ 2.2(c)(iii) *Laws Requiring Security Breach Notification of Affected Individuals*

Currently 47 states, as well as the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands, have responded to the increased threat of identity theft by enacting statutes requiring businesses to notify individuals whose personal information has been stolen.[26] Virtually all of these statutes have an impact on employers because they impose a duty to provide notice regardless of whether the personal information involved belongs to an employee or to a consumer. Only Alabama, New Mexico and South Dakota do not have a security breach notification law.

The notice of security breach statutes vary in detail from state to state but have substantial similarity in their broad outlines.

---

[24] 16 C.F.R. § 682.1(b).

[25] 16 C.F.R. § 682.3(a).

[26] ALASKA STAT. § 45.48.010; ARIZ. REV. STAT. ANN. § 18-545; ARK. CODE ANN. §§ 4-110-101 *et seq.*; CAL. CIV. CODE §§ 1798.29, 1798.80, 1798.82; COLO. REV. STAT. § 6-1-716; CONN. GEN. STAT. § 36a-701b; DEL. CODE ANN. tit. 6, §§ 12B-101 *et seq.*; D.C. CODE §§ 28-3851 *et seq.*; FLA. STAT. § 501.171; GA. CODE ANN. §§ 10-1-910 *et seq.*; HAW. REV. STAT. §§ 487N-1 *et seq.*; IDAHO CODE ANN. §§ 28-51-104 *et seq.*; 815 ILL. COMP. STAT. 530/5 *et seq.*; IND. CODE §§ 24-4.9-1-1 *et seq.*; IOWA CODE §§ 715C.1 *et seq.*; KAN. STAT. ANN. §§ 50-7a01 *et seq.*; KY. REV. STAT. ANN. § 365.732; LA. REV. STAT. ANN. §§ 51:3071 *et seq.*; ME. REV. STAT. ANN. tit. 10, §§ 1346 *et seq.*; MD. CODE ANN., COM. LAW §§ 14-3501 *et seq.*; MASS. GEN. LAW ch. 93H §§ 1 *et seq.*; MICH. COMP. LAWS § 445.72; MINN. STAT. § 325E.61; MISS. CODE ANN. § 75-24-29; MO. REV. STAT. §§ 407.1500.1 *et seq.*; MONT. CODE ANN. §§ 30-14-1704, 33-19-321; NEB. REV. STAT. §§ 87-801 *et seq.*; NEV. REV. STAT. §§ 603A.020 *et seq.*; N.H. REV. STAT. ANN. §§ 359-C:19 *et seq.*; N.J. STAT. ANN. § 56:8-163; N.Y. GEN. BUS. LAW § 899-aa; N.C. GEN. STAT. §§ 75-61, 75-65, 14-113.20; N.D. CENT. CODE §§ 51-30-01 *et seq.*; OHIO REV. CODE ANN. § 1349.19; OKLA. STAT. tit. 24, §§ 161 *et seq.*; OR. REV. STAT. §§ 646A.600 *et seq.*; 73 PA. CONS. STAT. §§ 2301 *et seq.*; R.I. GEN. LAWS §§ 11-49.3-1 *et seq.*; S.C. CODE ANN. §§ 39-1-90, 37-20-110 *et seq.*; TENN. CODE ANN. § 47-18-2107; TEX. BUS. & COM. CODE §§ 521.002 *et seq.*; UTAH CODE ANN. §§ 13-44-102 *et seq.*; VT. STAT. ANN. tit. 9, §§ 2430 *et seq.*; VA. CODE ANN. §§ 18.2-186.6, 32.1-127.1:05 (medical and insurance data); WASH. REV. CODE §§ 42.56.590, 19.255.010; W. VA. CODE §§ 46A-2A-101 *et seq.*; WIS. STAT. § 134.98; WYO. STAT. ANN. §§ 40-12-501 *et seq.*

- **Definition of Personal Information:** Various jurisdictions define *personal information* differently. For example:

- **Most jurisdictions:** define *personal information* to mean:

    1. an individual's name;

    2. accompanied by: (a) Social Security number, driver's license or state identification number, or (b) a financial account, credit or debit card number in combination with any security code or password that would permit access to the individual's financial account.

- **Illinois, Iowa, Nebraska, North Carolina, Texas and Wisconsin:** define *personal information* to include the above information as well as an individual's name accompanied by "unique biometric data such as a fingerprint, voice print, or retina or iris image, or other unique physical representation."[27]

- **Arkansas, California, Florida, Illinois, Missouri, Montana, Nevada, North Dakota, Oregon, Rhode Island, Texas and Virginia:** define *personal information* to include one or more of the following: an individual's medical history, mental or physical condition, medical treatment or diagnosis and/or an individual's health insurance policy number.

- **What Triggers the Notice Requirement?:** The obligation to notify affected individuals is triggered when the owner of unencrypted computerized data discovers, or is notified of, a security breach.[28] The laws include some limitations on the notice obligation. For example, in most states, notice is required only if the unauthorized acquisition causes, or is reasonably believed will cause, a material risk of identity theft or other fraud.[29] Moreover, the theft or loss of personal information that is encrypted generally will not trigger the notice obligation. In many states, an employer may avoid the notice requirements by redacting the personal information or taking other steps to make the information unreadable and unusable. Federally-regulated financial institutions and health care-related entities subject to regulation under HIPAA are usually exempt from the states' notice of security breach statutes, although such entities are required to provide notice under other federal laws.

- **Content of Notice:** Notably, a significant minority of these statutes mandates the content of the notice that must be provided to affected individuals. These content requirements can add significant variations to the notice requirements from state to state. In most circumstances, however, a notice of security breach may include the following:

    1. a brief explanation of the cause of the security breach;

    2. a description of the categories of information that were compromised;

    3. additional steps taken to safeguard the information;

---

[27] *See, e.g.*, IOWA CODE § 715C.1(11)(e);WIS. STAT. § 134.98(1)(b).

[28] In some states the notice obligation may be triggered even when data is not stored electronically. *See, e.g.*, ALASKA STAT. § 45.48.400; HAW. REV. STAT. ANN. § 487N-2(a); IND. CODE § 24-4.9-2-2 (*breach of security* includes "the unauthorized acquisition of computerized data that have been transferred to another medium, including paper, microfilm, or a similar medium, even if the transferred data are no longer in computerized format").

[29] In Massachusetts, businesses need not provide notice unless the security breach "creates a substantial risk of identity theft or fraud against a resident of the commonwealth." MASS. GEN. LAW ch. 93H, § 1.

4. steps that the recipient of the notice can take to reduce the risk of identity theft; and

5. a contact at the company who can provide assistance.

A notice that addresses all of these points likely will satisfy most state notice laws. Massachusetts, for example, additionally requires that the notice inform recipients of their right to obtain a police report and of the procedures for placing a security freeze on their credit reports.[30]

- **Procedural Requirements:** The notice in security breach statutes requires several procedural requirements.

  - Notice must be provided without unreasonable delay after the discovery of the security breach unless a law enforcement agency determines that notice would impede a criminal investigation or jeopardize national security—for example, because the notice would tip off a hacker under criminal investigation. The notice laws in Tennessee, Ohio and Wisconsin are unique in that they set a specific outside time limit—45 days from the date of discovery—for providing notice to individuals.[31]

  - In all states that have enacted security breach statutes, notice may be provided in writing or electronically under certain circumstances. Notice by telephone is permitted in approximately half of the states that have enacted notice of security breach statutes.[32]

  - The laws in several states require that the entity must also notify the three nationwide credit reporting agencies—the number of affected individuals that trigger this requirement varies by state.[33] Several states require that businesses provide notice of the breach to a state agency, typically the Attorney General's office. The number of affected state residents needed to trigger this requirement again varies.[34]

- **Multistate Employers:** State notice laws pose a particular challenge for multistate employers. Security breaches involving employee information typically do not affect just employees who reside in one state. The theft or loss of a backup tape containing payroll information, for example, generally will result in the unauthorized acquisition of personal

---

[30] MASS. GEN. LAW ch. 93H, § 3(b).

[31] *See, e.g.*, OHIO REV. CODE ANN. § 1349.19(B)(2); WIS. STAT. § 134.98(3).

[32] *See, e.g.*, ARIZ. REV. STAT. § 44-7501; COLO. REV. STAT. § 6-1-716(1)(c); CONN. GEN. STAT. § 36a-701b(e); DEL. CODE ANN. tit. 6, § 12B-101(3)(b); GA. CODE ANN. § 10-1-393.8; HAW. REV. STAT. ANN. § 487N-2(e); IDAHO CODE § 28-51-104(4); IND. CODE § 24-4.9-3-4; MD. CODE ANN. COM. LAW § 14-3504(e); MICH. COMP. LAWS § 445.72(5)(c) (if certain conditions are met); MISS. CODE ANN. § 75-24-29; MO. REV. STAT. §§ 407.1500.1 *et seq.* (if certain conditions are met); MONT. CODE ANN. § 30-14-1704(5); NEB. REV. STAT. § 87-802(3); N.H. REV. STAT. ANN. § 359-C:20(III); N.Y. GEN. BUS. LAW § 899-aa(5) (if certain conditions are met); N.C. GEN. STAT. § 75-65(e); OHIO REV. CODE ANN. § 1349.19(E); OKLA. STAT. tit. 24, § 162(7); OR. REV. STAT. § 646A.604(4); 73 PA. STAT. ANN. § 2302; S.C. CODE ANN. § 39-1-90; UTAH CODE § 13-44-202(5); VA. CODE ANN. §§ 18.2-186.6; VT. STAT. ANN. tit. 9, § 2435(b); W. VA. CODE § 46A-2A-102(d); WIS. STAT. § 895.507(3).

[33] *See, e.g.*, FLA. STAT. § 501.171(5); GA. CODE ANN. § 10-1-912(d) (if more than 10,000 residents are affected); MINN. STAT. § 325E.61(2) (if more than 500 residents are affected); N.Y. GEN. BUS. LAW § 899-aa(8) (if more than 5,000 residents are affected).

[34] *See, e.g.*, HAW. REV. STAT. § 487N-2(f); KY. REV. STAT. ANN. § 365.732; LA. ADMIN. CODE 16:III:701; N.Y. GEN. BUS. LAW § 899-aa(8); N.C. GEN. STAT. § 75-65(f). Under certain circumstances, notice also must be provided to consumer reporting agencies in Massachusetts and Montana. MASS. GEN. LAW ch. 93h, § 1; MONT. CODE § 30-14-1704(7).

information concerning employees in all of the employer's locations. In these circumstances, a multistate employer will be required to comply with the notice laws of every state in which affected employees reside. Given the variations of these laws in their details, multistate employers typically will need to confer with in-house or outside counsel who can ensure that the employer's response to the incident satisfies the varying requirements of each state that has enacted a notice law in which employees reside.

§ 2.2(c)(iv) *Other Legislative Efforts to Prevent Identity Theft*

- **Encryption of Transmitted Records:** Some states mandate encryption of transmitted records and stored data containing personal information.[35]

- **Security Freeze Laws:** All states and the District of Columbia have enacted "security freeze" laws to battle identity theft.[36] These laws permit an individual affected by a security breach to place a "freeze" on their personal credit records. The security freeze typically prohibits a consumer reporting agency from releasing all or part of the consumer's credit report or any information derived from it without the individual's express authorization. In any notice of security breach, employers should consider providing information on how affected employees can place a security freeze on their credit reports.

§ 3 GLOBAL INFORMATION SHARING: THE IMPACT OF INTERNATIONAL DATA PROTECTION LAWS ON MULTINATIONAL EMPLOYERS

§ 3.1 DISTINCTIONS IN GLOBAL APPROACHES TO PRIVACY

Multinational employers may centralize all personnel data in one location from locations around the world for record-keeping, benefits and payroll purposes, and this centralization raises issues regarding the affected nations' data protection laws. There are important distinctions between the privacy laws of the United States and other countries that must be taken into account whenever transferring employee data across national borders.[37]

A comparison of the United States's privacy framework with the European Union's comprehensive privacy regime highlights the significant differences between two global privacy models. Under the United States's sectorial approach, certain sectors of the economy are protected by privacy laws. For example, the medical industry is protected by the Health Information Portability and Accountability Act (HIPAA), and the banking and securities industry is protected by the Gramm-Leach Bliley Act (GLBA). Under this sectorial approach, no single authority is charged with enforcing and overseeing compliance with all privacy laws; instead, this responsibility is shared among a range of government agencies. For

---

[35] *See, e.g.*, *Frequently Asked Question Regarding 201 CMR 17.00*, MASSACHUSETTS OFFICE OF CONSUMER AFFAIRS & BUSINESS REGULATION, Nov. 3, 2009, *available at* http://www.mass.gov/?pageID=ocatopic&L=3&L0=Home&L1=Consumer&L2=Identity+Theft&sid=Eoca; *Nevada Personal E-Data Transfer Law Includes Mobile Devices, Encryption*, 8 PRIV. & SEC. L. REP. (BNA) 821 (June 8, 2009).

[36] National Conference of State Legislatures, *Consumer Report Security Freeze State Laws*, *available at* http://www.ncsl.org/default.aspx?tabid=12475.

[37] *See also* THE LITTLER MENDELSON GUIDE TO INTERNATIONAL EMPLOYMENT AND LABOR LAW (5th ed. 2017). This publication includes information on data protection laws of 60 countries and the European Union. *See* § 11.3 of each country-chapter for a discussion of data transfer restrictions.

example, the U.S. Department of Health and Human Services enforces HIPAA, while the U.S. Consumer Financial Protection Bureau enforces GLBA. The European Union's comprehensive data protection regime, on the other hand, protects all forms of *personal data*, defined as any information relating to an identified or identifiable natural person. Under the E.U. model, before personal data can be processed, which is defined to include collection, recording, storing, using or transferring the data outside of the European Union, the processing must comply with specific criteria. These criteria limit the situations in which an individual's personal data can be collected, used, or disclosed. For more information on the approach taken by the European Union, see **§ 3.1(b)**.

The varying approaches to data protections globally adds complexity and uncertainty to a corporation's best intentions to comply with applicable protections for employee information. Before undertaking a cross-border transfer of data, an employer must proactively ensure compliance with any pertinent data protection regime(s). The issues corresponding to any particular transfer will vary based on whether the transfer is to or from a country with strong privacy protections, such as those within the E.U. on the one hand, or to or from a country with little to no privacy protections in place.

To illustrate the challenges facing employers as a result of jurisdictional disparities, this section first discusses the general employment privacy regime and the obstacles confronted by companies and the approaches they utilize when transferring information or outsourcing administrative functions to countries with more established privacy regulatory schemes (*e.g.*, countries within the E.U.) and with limited protections (*e.g.*, China and India).

§ 3.1(a) *The U.S. Approach*

The United States uses a sectored approach to data protection, which relies on a combination of legislation and regulation at the federal, state and local levels, in addition to self-regulation. Employers in the United States should expect restrictions on data transfers imposed based on *ad hoc* factors. For example, in some instances, federal or state constitutions or statutes confer privacy protections based on location, such as in one's home.[38] In other instances, the United States' sectored approach provides protections based on the type of information. For example, the ADA and GINA impose strict limitations on the disclosure of employee health information, even within the corporate entity or to related entities. The United States' approach may also vary based on the reason for the collection.

§ 3.1(b) *The European Union Approach*

If a business's transborder data flow emanates from one of the Member States of the E.U.,[39] the organization will confront a markedly different approach to privacy and data protection than experienced in the United States.[40] In Europe, privacy is viewed as a fundamental human right. European countries have enacted comprehensive lawmaking to protect the privacy of individual citizens both at work and at home. European privacy laws generally apply to all forms of individually identifiable information and

[38] *See Griswold v. Connecticut*, 381 U.S. 479 (1965).

[39] The 28 Member States of the European Union are Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, The Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and (until "Brexit" is implemented) the United Kingdom. Under the European Economic Area (EEA) agreement, Iceland, Lichtenstein and Norway have implemented data protection laws similar to those in place in the Member States, although these countries are not members of the E.U.

[40] Many countries outside the E.U., including Argentina, Australia, Canada and the territory of Hong Kong, have enacted data protection laws based upon the European model. A discussion of the specific differences between the data protection laws of these countries and those applicable to the E.U. Member States is beyond the scope of this publication.

generally do not distinguish among various categories of information (*e.g.*, financial records, video rental information, model and color of a person's car, home address and telephone records), as is the case in the United States. While E.U. laws have enacted a baseline level of protection to all forms of individual information, the E.U. provides additional protections for certain categories of sensitive information, including medical records or information concerning one's sex life.

As applied to the employment context, multinational employers may not be able to apply standard U.S. business procedures to subsidiaries or related entities in the E.U. without due consideration. Where U.S.-based companies may ordinarily seek to obtain certain types of personal information from applicants or employees—such as national origin or even smoking status—obtaining certain categories of "sensitive personal data," such as race or ethnic origin, may be prohibited in the E.U. in certain circumstances. For example, a U.S. company motivated to increase diversity may ask for information related to one's age, race, national origin or other protected category; however, E.U. data protection laws impose strict limits on employers' collection of information concerning an employee's race or ethnic origin.

Monitoring e-mails presents a further example of enhanced privacy rights confronting employers in the E.U. While generally speaking, a U.S.-based multinational can transfer, without restriction, an employee's e-mail on the company's U.S. server to an E.U. subsidiary, the E.U. regulates a broader spectrum of information than the United States so that the disclosure of certain types of information permitted under U.S. law may not be permitted under the laws of other countries. To illustrate this point, in the E.U., the European Court of Human Rights awarded monetary damages to an employee when her employer, a college in Wales, monitored her e-mail account without her knowledge.[41] The court ruled that the college's surreptitious monitoring of the employee's e-mail activities "amounted to an interference with her right to respect for her private life and correspondence," despite the fact that the college owned the computers and e-mail accounts through which the communications had been transmitted.[42] Furthermore, in a 2013 decision, the Brussels Labour Court of Appeal refused to admit a former employee's e-mails into evidence to establish the employer's justification for the employee's termination because the employer's actions in reviewing the employee's e-mails violated E.U. and Belgian privacy rules.[43]

§ 3.1 (b)(i) *Works Councils*

One selective area of added privacy protections in the E.U. may apply to employers. Specifically, the E.U. Works Council Directive imposes a duty upon certain large employers with 1,000 or more E.U. employees and at least 150 employees in two or more Member States to inform and/or consult with a *works council*—that is, an organized panel of plant-level employees—before making decisions that touch upon the privacy rights of its workers.[44] Another directive aimed at employers with only 20 or 50 employees in the E.U., depending upon the choice made by a Member State, discusses national works councils and the adoption of certain minimum standards on consultation and the sharing of information between management and workers.[45] Although the subjects upon which the company must confer with a

---

[41] *See Case of Copland v. United Kingdom*, No. 62617/00 (E.C.H.R. Apr. 3, 2007).

[42] *See Case of Copland v. United Kingdom*, No. 62617/00, at 44 (E.C.H.R. Apr. 3, 2007).

[43] Phillipe Francois & Julien Hicks, *Netherlands: Brussels Labour Court of Appeal Disallows Use Of E-Mails Obtained In Violation Of The Privacy Rules*, MONDAQ.COM, Mar. 26, 2013, *available at* http://www.mondaq.com/404.asp?404;http://www.mondaq.com:80/x/229022/employment+litigation+tribunals/brussels-labour-court/brussels-labour-court-1.jpg&login=true.

[44] Council Directive 2009/38/EC of 6 May 2009 on the Establishment of a European Works Council or a Procedure in Community-Scale Undertakings and Community-Scale Groups of Undertakings for the Purposes of Informing and Consulting Employees, O.J. (2009) L 122, art. 2.

[45] Council Directive 2002/14/EC of 11 March 2002 Establishing a General Framework for Informing and Consulting Employees in the European Community, O.J. (2002) L 80, art. 2.

works council vary with each Member State, these subjects often include collection of employee data, data protection policies, employee monitoring policies, implementation of new technologies in the workplace and transfers of employee information to foreign affiliates.

Consultation with a works council may be a lengthy and arduous process and require formalized documentation in certain circumstances. However, in most E.U. Member States—Germany excluded—the positions taken by works councils are nonbinding and do not limit the actions that the company ultimately may take.[46] Nevertheless, consultation with works councils is not a voluntary exercise, and failure to do so may result in negative publicity and damage to a company's goodwill with its employees.

§ 3.1(c) *The Latin American Approach*

Eleven countries throughout Central and South America have adopted data privacy regulations: Argentina, the Bahamas, Chile, Colombia, Costa Rica, Mexico, Nicaragua, Peru, Saint Lucia, Trinidad and Tobago and Uruguay.[47] Several of these regulations involve similar requirements as E.U. and U.S. data protection regulations. For example, Colombia, Costa Rica, Nicaragua, Peru, and Trinidad and Tobago have established data protection authorities responsible for overseeing compliance with the data protection laws. Several other laws regulate the appropriate manner for transferring documents and providing notice to individuals of that transfer. Unlike the E.U., however, there is no common directive for the data protection laws in Central and South America. Because of this, employers must interpret each country's data protection laws individually.

§ 3.2 E.U. DATA PROTECTION DIRECTIVE & THE UPCOMING GENERAL DATA PROTECTION REGULATION

Following the formal adoption of the Data Protection Directive 95/46/EC ("Directive") on October 24, 1995, each E.U. member state was responsible for enacting its own laws that implemented the fundamental principles of the Directive. This resulted in considerable differences in the data protections laws of each member state, causing legal uncertainty and significant administrative costs and burdens for companies. To address those issues, on December 15, 2015, the European Parliament, Council and Commission agreed to new data protection rules introduced as the General Data Protection Regulation (GDPR) that will repeal and replace the Directive.[48] The GDPR passed its final legislative hurdle when it was adopted by the European Parliament on April 14, 2016. The GDPR went into effect on May 24, 2016 with its publication in the *Official Journal of the European Union*, and all E.U. Member States will have to be in compliance with the GDPR by May 25, 2018.

The GDPR establishes a harmonized data protection framework across the E.U. that is intended to make the rules for companies more uniform and to strengthen citizens' fundamental rights. Once fully implemented, the GDPR should eliminate country-specific differences in data protection requirements that increase compliance burdens, although local labor laws still could result in country-specific requirements for the processing of employees' personal data.

---

[46] 182 Lab. Rel. Rep. 448 (Nov. 5, 2007).

[47] *Privacy in Latin America*, BNA PRIVACY & SEC. L. REP., *available at* http://privacylaw.bna.com/pvrc/7057/split_display.adp?fedfid=29020883&vname=pvlrnotallissues&fn=29020883&jd=29020883.

[48] *Commission Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, COM (2012) 11 final (Jan. 25, 2012), *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=en.

§ 3.2(a) *E.U. Data Protection Directive's Application to Employment Law*

Until the GDPR takes effect in May 2018, the 1995 Directive sets the minimum standards for the applicable law in the European Union. The Directive's objectives are twofold:

1. to protect individuals with respect to the processing of personal information; and

2. to ensure the free movement of personal information within the E.U. through the coordination of national laws.

The Directive is broad in scope. It encompasses all categories of individually identifiable personal information, not just discrete categories of personal data, such as health or financial information.[49] Employee personnel information is covered, including names, addresses, phone numbers, gender type, employee identification numbers, resumés, educational histories, e-mail addresses, pay rates, benefits, performance reviews and training records. The Directive applies to all forms of *data processing*—which is defined to include all functions with respect to personal data, such as collection, use, disclosure, storage and destruction—whether online or offline, manual or automated. This term excludes only processing "in the course of purely personal or household activity."[50] In its first decision addressing application of the Directive, the Court of Justice of the European Communities construed this exemption narrowly, holding that the posting by a church volunteer of a web page containing personal information about other church members fell outside the exemption because this activity "clearly extended beyond [the volunteer's] personal and domestic circle."[51]

The fundamental principles of the Directive, as applied to the employment context, include the following:

- **Legitimacy:** The employer (the "data controller") may process an employee's (the "data subject's") personal data only: (1) with the employee's prior consent; (2) as necessary to perform the employment contract; (3) to the extent necessary to comply with legal obligations; or (4) for other legitimate interests of the employer.

- **Notice or Transparency:** Before processing personal data, the employer must inform the employee of the personal data being collected, how and why the personal data has been or will be processed, to whom the data has been or will be disclosed and whether the data will be exported outside the E.U.

- **Proportionality:** The employer may process data for the purposes disclosed in the notice to employees, or for compatible purposes. The personal data which is processed under the Directive must be the minimum necessary to carry out that purpose. It would violate this "minimum necessary" requirement, for example, to require that a job applicant furnish his or her prospective employer with the European equivalent of a Social Security number, if that number would not be used in the hiring process.

- **Access:** The employer must: (1) grant each employee's reasonable request for access to the personal data it maintains; (2) provide each employee with the opportunity to correct, erase or block further processing or transfers of inaccurate, outdated or incomplete data; and (3) notify any third party to whom inaccurate, outdated or incomplete data has been disclosed of any additions or corrections made in response. While some *ad hoc* U.S. federal or state authority

[49] O.J. (1995) L 281, 31, art. 2.

[50] O.J. (1995) L 281, 31, art. 3.

[51] *Criminal Proceedings Against Lindqvist*, Case C-101/01, at 34 (E.C.J. Nov. 6, 2003).

provides employee access to some employee documents (such as personnel files),[52] the scope does not approach the access requirements in the Directive.

- **Security:** The employer must implement technical and organizational safeguards to protect the data from unauthorized access and disclosure. These types of security are often imposed in the U.S. based on the type of information, if, for example, it is medical information.

- **Accuracy:** The employer must take steps to ensure that personal data is accurate and up-to-date.[53]

The Directive requires each E.U. Member State to enact implementing legislation that incorporates the Directive's guiding principles into the Member State's own national laws. The Directive further requires that each Member State establish a "data protection authority," an administrative agency responsible for enforcing the laws implemented in the Member State to effectuate the Directive's guiding principles.[54] Before processing any personal data, the national data controller generally is required to notify the local data protection authority of that processing through a public filing.[55]

§ 3.2(b) *E.U. General Data Protection Regulation's Application to Employment Law*

Only one of the GDPR's 91 articles specifically addresses the personal data of prospective, current or former employees (collectively, "employee data"). Article 81 of the version published by E.U. authorities in December 2015 provides that E.U. Member States may enact laws specific to the processing of employee data to implement the GDPR. For multinational employers, this provision could defeat one of the principal putative benefits of the GDPR—to establish a single set of data protection rules applicable in all E.U. Member States to eliminate complexity, ensure consistency and reduce administrative costs. In respect of employee data, the GDPR should therefore be read in conjunction with any applicable laws of relevant E.U. Member States that regulate the handling of employee data.

Even though the GDPR specifically addresses employee data in only one article, the GDPR applies broadly to the processing of all "personal data," which is defined to mean "any information related to an identified or identifiable natural person." Consequently, U.S. multinationals need to determine how to apply, in the employment context (together with the applicable local employee data protection laws), regulatory requirements designed to protect online consumers and numerous other categories of data subjects.

The GDPR's scope is broad in another way that impacts U.S.-based multinationals. The GDPR applies to all E.U. residents, regardless of citizenship. For U.S.-based multinationals, this means that expatriates working at an E.U. subsidiary are entitled to all of the GDPR's protections when their data is collected while they reside in the European Union.

Additional highlights from the GDPR that multinational employers should consider include:

---

[52] *See e.g.*, CAL. LAB. CODE § 1198.5.

[53] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, O.J. (1995) L 281, 31, arts. 6–7.

[54] O.J. (1995) L 281, 31, art. 28.

[55] O.J. (1995) L 281, 31, art. 18.

- Employers can only "process" employee data if the GDPR specifically permits the processing.

- The GDPR requires that data controllers distribute a notice of data processing to each individual when personal data is first collected. As applied in the employment context, this means that employers will be required to provide a notice to job applicants concerning the processing of their data during the application process as well as a notice to new hires, typically during the onboarding process, explaining how their personal data will be processed during the employment relationship.

- While the basic notification requirement is unchanged from the Data Protection Directive, the GDPR requires a far more robust notice. The notice must include the following information: (1) the identity and contact details of the employer; (2) the purposes for the processing and when the processing is based on legitimate interests, a description of those interests; (3) the categories of recipients of disclosures of personal data; (4) that the controller intends to transfer personal data to a third country and the legal basis for the transfer ; (5) the period for which the personal data will be stored or the criteria for determining the period; (6) how employees can exercise the rights of access, correction, erasure and objection; (7) where processing is based on consent, the right to withdraw consent; (8) the right to file a complaint with a data protection authority (DPA); (9) whether the employee is obliged to provide the data by statute, contract or for another reason, and the possible consequences of failing to provide the data; and (10) whether the personal data will be subject to automated processing and, if so, the logic and consequences of the processing for the data subject.

- The GDPR places substantial emphasis on individuals' rights of access, correction, erasure and objection as a means of achieving the new law's broader objective of protecting individuals' fundamental right of privacy. To that end, the GDPR requires that employers provide employees with a mechanism to exercise these rights and to respond, in writing, to any request without undue delay and, at the latest, within one month. The response period may be extended for up to two additional months in light of the complexity and number of requests. Any denial of a request must include the reasons for the denial and the right to file a complaint with the DPA or to seek judicial relief. All responses to requests must be free of charge unless the request is manifestly excessive (generally because it is repetitious). If the employer has doubts regarding the identity of a person making a request, it may ask for verification of the person's identity.

- While prior law provided a right of access and correction, the right of erasure (also known as the "right to be forgotten") is new. Employees generally have the right to require the employer to delete their personal data when, for example: (1) the data no longer is necessary for the purposes for which it was collected; (2) the employee has withdrawn consent to processing, and no other ground for processing is available; and (3) the employee objects to processing, and there is no compelling ground that overrides the employee's interests. However, employers are not required to erase any employee data that they are required to retain under E.U. or Member State law that is necessary to establish, pursue or defend legal claims.

- The GDPR requires employers to implement administrative and technical safeguards for employee data to reduce identified risks and to prevent a "personal data breach." The GDPR defines a breach to mean a "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data." The GDPR does not specify safeguards that must be implemented, but it identifies the following

steps and objectives as potentially appropriate: (1) pseudonymization and encryption; (2) the ability to ensure the confidentiality, integrity and availability of personal data; (3) disaster recovery capabilities; and (4) a process for regularly testing, assessing and evaluating the safeguards.

- When a personal data breach occurs, the GDPR requires prompt action. The employer must notify the DPA within 72 hours, and if that notification is delayed, explain the reason for the delay. Notification is not required if the breach "is unlikely to result in a risk for the rights and freedoms of individuals." The employer must document its breach response sufficiently to permit the DPA to verify compliance with the GDPR.

- Employers must notify affected employees of a personal data breach "without undue delay," if the breach is "likely to result in a high risk to the rights and freedoms of individuals," or if ordered to do so by the DPA. As with U.S. breach notification laws, the GDPR establishes an "encryption safe harbor," meaning that the employer is not required to notify affected individuals if their personal data is subject to encryption that renders the information unreadable. Notification to individuals also is not required if: (1) the employer took steps to ensure that the high risk to employees does not materialize; or (2) notification would involve disproportionate effort, but in this case, the employer must provide notice by public communication, such as by posting notice on a website or by publication in the media.

- The GDPR specifies a long list of matters that must be addressed in the service agreements with vendors that access personal data from Europe. The service agreement must address, for example: (1) the subject matter and duration of the processing; (2) the nature and purpose of the processing; and (3) the types of personal data and categories of data subjects. The service agreement also must impose numerous obligations on the service provider, including, for example, that the service provider: (1) process personal data only subject to the employer's instructions; (2) require its employees to execute a confidentiality agreement; (3) implement required security measures; (4) assist the employer fulfill its obligations to respond to requests by employees to exercise their rights; and (5) cooperate with the employer in fulfilling its breach notification obligations.

- The GDRP provides that the processing of "special categories of personal data," also known as "sensitive personal data," is prohibited unless an exception applies. Sensitive personal data includes race or ethnic origin, data concerning health or sex life and sexual orientation, trade-union membership, genetic data, biometric data, political opinions, and religious or philosophical beliefs. An employer can process sensitive personal data only in the following limited circumstances: (1) the employee gives explicit consent (except where the law does not permit the employee to consent); (2) processing is necessary for the employer to fulfill obligations and exercise specific rights established by E.U. or Member State law; or (3) processing is necessary to establish, pursue or defend against legal claims. In addition, a health care professional can process personal data concerning an employee's health when necessary for preventive or occupational medicine, to assess the working capacity of the employee or to provide care. Given the GDRP's emphasis on protecting sensitive personal data, regulators likely will narrowly construe these exceptions. The GDPR also establishes a special rule for the processing of criminal history information, albeit that category is not specifically identified as sensitive personal data. Under that special rule, an employer can process criminal history information— even with an applicant's or employee's consent—only if specifically authorized by E.U. or Member State law to perform a criminal history check.

- The GDPR requires that employers maintain detailed records concerning their data processing. These records must be provided to the DPA upon request. The information to be recorded includes the following: (1) contact information for the employer; (2) the purposes of the processing; (3) the categories of data subjects and of personal data processed; (4) the categories of recipients, including those in third countries; (5) the third countries to which personal data will be transferred and the instrument, *e.g.*, Standard Contractual Clauses (SCCs) approved by the European Commission or binding corporate rules (BCRs) used to provide an adequate level of protection; (6) where possible, the envisaged retention periods for different categories of employee data; and (7) a general description of the security measures for employee data.

Overall, the GDPR will not demand dramatic changes in the policies and procedures previously implemented to comply with the Directive. While the compliance requirements have not changed significantly, the enforcement risk has increased dramatically. The GDPR empowers data protection regulators to impose administrative fines of 20 million Euro, or up to 4% of a corporate group's worldwide gross annual revenue, for most violations and up to 2% of that amount, or 10 million Euro, for less serious violations. Regulators also can ban data processing at the E.U. subsidiary and suspend data transfers to the parent corporation. Consequently, U.S.-based multinationals should take advantage of the two-year grace period to come into compliance.

§ 3.2(c) *Transfer of Data to the United States & Other Countries*

Of particular significance for U.S. employers with employees in the E.U., personal data generally cannot be transferred from an E.U. Member State to a country outside the E.U. unless the "data exporter" first obtains the approval of the national data protection authority. Approval may be denied if the recipient of the personal data resides in a country that does not provide "an adequate level of protection," meaning privacy protections similar to, or more stringent than, those required by the Directive.[56]

The "adequacy" standard creates a potential barrier to data exports from the E.U. to the United States. The European Commission, the E.U.'s executive body, has determined that United States privacy law does *not* provide "an adequate level of protection." National data protection authorities can rely upon that determination to block data exports to the United States and to seek administrative penalties from, and criminal prosecution of, those who intentionally circumvent this restriction.

§ 3.2(c)(i) *Invalidation of U.S. – E.U. Safe Harbor Framework & Adoption of the Privacy Shield*

Until October 2015, multinational employers could rely on a Safe Harbor Framework, an agreement forged years ago between the U.S. Department of Commerce and the European Commission to permit the transfer of personal data. In 2000, the Commission ruled that the Safe Harbor Framework would meet the "adequate level of protection" standard.[57] Under the Framework, U.S. businesses wishing to receive personal data from the E.U. were required to: (1) post a Safe Harbor Privacy Policy in which they represented their intention to adhere to seven Safe Harbor Principles designed to protect the data;[58] (2)

[56] O.J. (1995) L 281, 31, arts. 18, 25–26.

[57] Decision 2000/520/EC of the European Court of Justice of 26 July 2000 on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce.

[58] The seven principles addressed: (1) notice; (2) choice (*i.e.*, affirmative consent or opportunity to "opt out" of information's disclosure); (3) transfer rules related to a third-party nonagent; (4) security; (5) data integrity; (6) access; and (7) enforcement.

submit a self-certification form through the Commerce Department's Safe Harbor website; and (3) pay a required fee.[59] The FTC had responsibility for enforcing the Safe Harbor Framework.[60]

In October 2015, the E.U. Court of Justice (ECJ) invalidated the Safe Harbor Framework. The ECJ held that the Safe Harbor Framework did not ensure an "adequate level of protection" for personal data because of lack of meaningful enforcement by the FTC, access to personal data by intelligence agencies (highlighted by Edward Snowden's leaks demonstrating that U.S. intelligence agencies are permitted to collect substantial quantities of personal data) and the inability of E.U. citizens to seek administrative or judicial redress for the collection of their personal data under U.S. surveillance programs.[61]

The invalidation of the Safe Harbor Framework caused a radical structural change in the relationship between the European Union and the United States as it pertains to cross-border data transfers. Before the ECJ's ruling, more than 4,000 U.S. businesses had relied on the Safe Harbor to legitimize cross-border data transfers. As a result, the group of European data protection regulators from each of the 28 E.U. Member States, known as the Article 29 Working Party, were under pressure to issue guidance on the implications of the ECJ's decision.[62] On February 2, 2016, E.U. and U.S. negotiators announced the outline of the "Privacy Shield" as the new framework for trans-Atlantic data transfers.[63] The European Commission issued its determination that that the Privacy Shield provides an "adequate level of protection" on July 12, 2016, and the Privacy Shield went into effect on August 1, 2016. The Privacy Shield is in many ways similar to the invalidated Safe Harbor.

Because of continued uncertainty over the Privacy Shield, however, U.S.-based multinationals should remain vigilant in monitoring developments. Notably, when the European Union's top data protection regulatory body, the Article 29 Working Party (the "Working Party"), completed its initial review of the proposed Privacy Shield, it expressed "strong concerns" with the new framework.[64] The European Data Protection Supervisor followed with a lengthy critique of the Privacy Shield in June 2016. These critiques, therefore, provide a playbook for a legal challenge to the Privacy Shield. The Privacy Shield may also be materially revised in the future based on these critiques. For example, the Article 29 Working Party raised concerns that the Privacy Shield does not provide an adequate level of protection as required by the GDPR. Furthermore, there is currently more than one pending lawsuit challenging the Privacy

---

[59] Information on the Safe Harbor Framework can be found at the Commerce Department's website (http://export.gov/safeharbor/).

[60] Since 2009, the FTC has initiated enforcement actions alleging that companies had deceptively held themselves out to be in compliance with the Safe Harbor. *See* Federal Trade Comm'n, Press Release, *FTC Settles with Six Companies Claiming to Comply with International Privacy Framework* (Oct. 6, 2009), *available at* http://www.ftc.gov/opa/2009/10/safeharbor.shtm; *see also* Federal Trade Comm'n Enforcement of Safe Harbor Commitments, *available at* http://export.gov/build/groups/public/@eg_main/@safeharbor/documents/webcontent/eg_main_052211.pdf.

[61] Other countries, both inside and outside the European Union acted to revoke their safe harbors after the European Union acted, including Switzerland, Israel, Dubai, Portugal and Spain.

[62] Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems) (Nov. 6, 2015), *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2015:566:FIN; *see also* European Comm'n, Press Release, *Commission Issues Guidance on Transatlantic Data Transfers and Urges the Swift Establishment of a New Framework Following the Ruling in the Schrems Case* (Nov. 6, 2015), *available at* http://europa.eu/rapid/press-release_IP-15-6015_en.htm.

[63] European Comm'n, Press Release, *EU Commission and United States Agree on New Framework for Transatlantic Data Flows: EU-US Privacy Shield* (Feb. 2, 2016), *available at* http://europa.eu/rapid/press-release_IP-16-216_en.htm.

[64] Statement of the Article 29 Working Party on the Opinion on the E.U.-U.S. Privacy Shield (April 13, 2016).

Shield. It is unclear at this time whether the European Commission is planning to address concerns by revising the Privacy Shield.

Consequently, employers need to decide whether to adopt the Privacy Shield (see **§ 3.2(c)(ii)**) or turn to one of two long-standing alternatives to the Privacy Shield and Safe Harbor certifications (see **§ 3.2(c)(iii)**). To make this decision, employers should consider undertaking a thorough (and privileged) review of their current data protection practices for E.U. employees' personal data and evaluate the available options for such data transfers moving forward. A description of the Privacy Shield, as well as long-standing alternatives to the Privacy Shield and Safe Harbor certifications, are discussed immediately below..

§ 3.2(c)(ii) *U.S. – E.U. Privacy Shield*

As with the Safe Harbor, the basic steps necessary to enjoy the Privacy Shield's benefits are straightforward. An eligible U.S. organization[65] must self-certify on the Commerce Department's Privacy Shield website and publish a Privacy Shield Privacy Policy that embodies the Privacy Shield Privacy Principles. U.S. organizations were able to self-certify beginning August 1, 2016.

Self-certifying for transfers of human resources (HR) data in the context of the employment relationship is substantially the same as self-certifying for transfers of other types of personal data. The organization will be required to provide basic information, including, for example, the organization's contact information, information about the data transfer and information about the organization's privacy policy. A corporate officer must sign the self-certification form.

Self-certification for transfers of HR data entails one critical distinction from other types of data transfers. The organization is required to choose E.U. data protection authorities (DPAs) from among the several available independent dispute resolution mechanisms. In addition, organizations must pay a fee that will not exceed $500 dollars, and will be less for smaller companies, to subsidize this dispute resolution mechanism.

The "human resources privacy policy" submitted with the self-certification must contain the same mandatory elements as other Privacy Shield privacy policies. The policy must address the organization's commitment to all seven of the "Privacy Shield Privacy Principles" (the "Principles"). These Principles include Notice, Choice, Accountability for Onward Transfers, Security, Data Integrity and Purpose Limitation, Access, and Recourse/Enforcement and Liability. To satisfy the Commerce Department that the HR privacy policy fully addresses the Principles, the policy submitted by the certifying organization must contain a long list of required elements including, among others:

1. an identification of all U.S. affiliates that will access transferred personal data and their commitment to adhere to the Principles;

2. the categories of personal data collected;

3. the purposes for the collection;

4. the third parties to which data may be transferred;

5. a description of data subjects' access rights; and

[65] The certifying entity must be subject to the jurisdiction in the United States of either the FTC or the Department of Transportation.

6. a contact for requests to exercise individual rights and submit complaints.

There is one significant distinction between an HR privacy policy and privacy policies addressing other types of personal data under the Privacy Shield. The HR privacy policy does not have to be posted on a publicly available website. Instead, the policy must be posted where it will be available to all E.U.-based employees whose personal data will be transferred to the U.S. subject to the Privacy Shield. This typically means that the policy will be posted on the corporate intranet. Organizations that choose not to publicly post their HR privacy policy will be required to submit the policy with the self-certification form rather than just providing a link.

Once the certifying organization completes these basic steps, the Commerce Department will review the self-certification form, to confirm that required information has been provided, and the HR privacy policy, to confirm that it addresses all required elements. If so, the Commerce Department will list the U.S. parent corporation and any certifying affiliates on its Privacy Shield List. Immediately after the listing, the E.U. subsidiaries can begin transferring their employees' personal data to the U.S. Because the European Commission has determined that the Privacy Shield "ensures an adequate level of protection for personal data," the E.U. subsidiaries will not need to obtain additional approvals from local DPAs, albeit in some countries, such as France, the DPA must be notified of the data transfer.

The Privacy Shield can be used to transfer personal data of both current and former E.U. employees. The U.S. parent corporation must apply the Principles to all transferred data for as long as that information is retained, even if the parent corporation subsequently decides to withdraw from the Privacy Shield. An organization that withdraws from the Privacy Shield will be required to satisfy the annual verification and recertification requirements for as long as the organization retains personal data transferred pursuant to the Privacy Shield.

Additional information on the Privacy Shield and the steps that an employer should consider taking to implement a Privacy Shield compliance program are discussed at **§ 4.2**.

§ 3.2(c)(iii) *Continued Alternatives to the Privacy Shield Certification*

Two principal alternatives are available to the Safe Harbor and Privacy Shield certifications, each of which presents its own challenges. Employers can consider using the "Standard Contractual Clauses" (SCCs) approved by the European Commission or relying on binding corporate rules (BCRs). There are also certain exceptions to the Data Protection Directive, referred to in E.U. parlance as "derogations," that may apply in the employment context.

Standard Contractual Clauses

SCCs (also referred to as "Model Clauses") remain a valid mechanism for transferring personal data outside the E.U. The SCCs are sets of model contract clauses embedded in a data transfer contract that the Commission has determined ensure an adequate level of protection for transferred personal data. Two sets of the clauses relate to the transfers between controllers, such as transfers between E.U. subsidiaries and their U.S. parent corporation, while another clause addresses transfers between a controller and a processor, such as transfers between an employer and a service provider.

In an implicit rebuke to some national data protection authorities who have questioned the continued viability of the SCCs after the ECJ's decision, the Communication states that national data protection authorities "may not refuse the transfer of [personal] data to a third country on the sole basis that these

SCCs do not offer sufficient safeguards."[66] However, the Commission acknowledges that national data protection authorities may continue to require submission of the SCCs for review to confirm that none of the standard clauses have been modified. The E.U. countries where Model Contracts must be submitted for review include, for example, Austria, France, Portugal, Romania and Spain.

In addition to the potential delay caused by this review, SCCs can also be unwieldy, administratively burdensome and slow to implement. The parties to these agreements cannot modify the SCCs, in any respect, to address any factual circumstances specific to their relationship. In addition, the parties are required to complete a form appendix to the SCCs that describes the data transfer in substantial detail, including the categories of data to be transferred and the purposes for which the transferred data will be processed. When the data importer needs to import additional categories of personal data or use the personal data transferred for new purposes, the appendices to the data transfer agreements must be amended. When a U.S. multinational has a large number of EU subsidiaries, managing these agreements and the amendments to them can be administratively burdensome.

Binding Corporate Rules

BCRs provide another alternative mechanism to the Safe Harbor for transfers of personal data within a corporate group. BCRs involve the development and implementation of a uniform set of rules that provide the high level of protection for personal data required by the Directive and are binding on all members of the corporate group, regardless of location.

While BCRs may initially appear to be a ready-made solution for U.S. multinationals that previously relied on Safe Harbor certification, they likely will not provide the answer for most companies. Notably, since the Commission first approved BCRs in the early 2000s, fewer than 100 companies globally and fewer than 30 in the U.S. have implemented them.[67] Those organizations that have implemented BCRs are among the largest, richest and most sophisticated U.S. corporations. BCRs likely have been selected by so few organizations (as compared to the more than 4,000 organizations certified to the Safe Harbor) because of the onerous approval process. The data protection authority of each country where the U.S. organization has a subsidiary with employees is entitled to an opportunity to review and comment on the BCRs. Additionally, the Conference of German Data Protection Authorities issued guidance that, for now, German data protection authorities will not approve BCRs.[68]

This review and approval process can require substantial resources to navigate and routinely takes more than one year to complete. Moreover, with the invalidation of the Safe Harbor, many data protection authorities likely will see a spike in requests for approval of BCRs, resulting in additional delay. With the low cost and ease of trans-Atlantic telecommunications, many smaller U.S. companies are now multinational employers. These companies typically will not have the internal resources, financial capital or time to complete the BCR review and approval process.

Derogations

As with most legal rules, the Directive sets out several exceptions (or "derogations") to the general rule that personal data cannot be transferred to a third country unless that country "ensures an adequate level

[66] Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems) (Nov. 6, 2015).

[67] *See* Information Commissioner's Office, *Binding Corporate Rules*, *available at* https://ico.org.uk/for-organisations/binding-corporate-rules/.

[68] Positionspapier der DSK, Sondersitzung der DSK am 21. Oktober 2015 in Frankfurt.

of protection" for personal data. The November 2015 Communication from the European Commission highlights the relatively limited value for employers of the derogations as an alternative to the Safe Harbor. The only two derogations potentially applicable in the employment context are: (1) transfers with the unambiguous consent of the data subject (*i.e.*, the employee); and (2) transfers that are necessary for the performance of a contract between the data subject (*i.e.*, employee) and the controller (*i.e.*, the E.U.-based employer). On the first, the Communication echoes the commonly held view that employers generally cannot rely on employees' consent to transfer personal data outside the EU because of "the relationship of subordination and inherent dependence of employees."[69] As a result, employees' consent generally cannot be "freely given," which is required for consent to be valid.

For the second, "performance-of-contract" derogation to apply, the Commission explains that "there has to be a 'close and substantial connection,' a 'direct and objective link' between the data subject and the purpose of the contract."[70] In other words, a multinational employer might be able to rely on this derogation to justify transfers of personal data if needed to administer payroll. However, the E.U. subsidiary/employer likely would not be able to rely on this derogation to justify the parent corporation's use of E.U. employees' personal data for purposes less tightly tied to performance of the employment agreement between the E.U. employee and the E.U. subsidiary, such as global diversity initiatives, global training programs or global succession planning.

§ 3.2 (d) *Role of Brexit*

It remains to be seen how the United Kingdom's decision to exit the European Union will influence the transfer of personal data and requirements for multinational employers. Once the United Kingdom leaves the European Union, it will no longer be required to align its data protection laws with the GDPR. However, it may be within its interest to do so to facilitate transfers of personal data from the European Union to the United Kingdom. For example, if the United Kingdom were to join the European Economic Area (such as Norway, Lichtenstein and Iceland), it would be required to continue to comply with the GDPR, and there would be no restrictions on cross-border data transfers. Alternatively, the United Kingdom may seek an adequacy determination from the European Commission, similar to the arrangement entered into with Switzerland. This would require a finding that the United Kingdom's data protection laws provide an adequate level of protection. If the Commission were to issue such a determination, it would allow the free transfer of personal data between the United Kingdom and the European Union.

The United Kingdom has been following E.U. data protection regulations for 15 years, so it is likely that the European Commission would make a determination that the United Kingdom's data protection laws (unless drastically modified post-Brexit) provide an adequate level of protection. That said, U.S.-based companies with operations in the United Kingdom should assess whether there are significant transfers of personal data from Member States to the United Kingdom. Companies should also watch for guidance from E.U. regulators regarding compliance with the GDPR and examine any existing model contracts and binding corporate rules addressing data transfers to assure compliance and accuracy.

---

[69] Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems) (Nov. 6, 2015).

[70] Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems) (Nov. 6, 2015).

§ 3.3 SAFEGUARDING PRIVATE INFORMATION IN COUNTRIES WITH LESS ESTABLISHED PRIVACY PROTECTION SCHEMES

Operating between or among jurisdictions with well-established privacy regimes such as the European Union and United States can cause multinational companies to grapple with harmonizing and interpreting privacy laws. In the alternative, companies may choose to expand into countries with lesser workforce protections than the United States and the European Union. Avoiding conflicts between the existing privacy laws of more developed jurisdictions is one reason to outsource administrative functions and/or expand business into areas with less developed privacy laws. Outsourcing into these areas may also be induced by rapid expansion, the desire for cost savings, staffing shortages or any number of other reasons.

Regardless of the reason, such an expansion will in some instances lead to the international transfer of private employee data from a more-regulated area to a less-regulated area. In the absence of applicable laws in jurisdictions with undeveloped privacy protections, the preservation of employee privacy likely will result principally from the measures a company takes to safeguard the security of personal data.

In jurisdictions with less-developed privacy regulations, there may be little or no recourse for the disclosure of information. However, even if a foreign host does not provide an adequate remedy, the disclosure of private employee information by employees in other countries has the potential to create liability in the United States under the theories of agency and/or vicarious liability, among others.[71] Thus, companies cannot consider outsourcing a "race to the bottom" in terms of seeking the lowest required privacy protections. To the contrary, as between two jurisdictions, a company often will be required to contractually ensure that personal data transferred to the jurisdiction with the less stringent requirements continues to receive the safeguards mandated by the jurisdiction with the more stringent requirements.

While not an exhaustive list of actions to be taken, the following are some proactive steps that a company can take to heighten safeguards for the personal data that is transferred to an offshore outsourcer:

- **Contractual Arrangements.** Contractual arrangements with any third-party provider, contractor, or employee can put in place the needed confidentiality conditions to comply with applicable regulations. Contracts between a foreign contractor or other third-party provider can specify a contractual remedy that requires the posting of a bond, for example, to secure recovery in the event information is compromised. By listing specific laws or regulations and requiring acknowledgement, companies can require foreign employees, contractors, or other third-party providers to expressly acknowledge the existence and applicability of laws or regulations, and can require their agreement to abide by the laws or regulations. Other contractual arrangements can include choice-of-law and choice-of-forum provisions specifying that any matter shall be tried in the United States and subject to U.S. law. Alternatively, the arrangement can require adjudication outside of the United States, provided that laws of another jurisdiction, such as the United States, will be applied. Finally, a contract can also require a private form of dispute resolution, such as binding arbitration that can be adjudicated under specified privacy laws. In this way a company can individually agree to privacy protections in order to fill the regulatory vacuum of less-regulated jurisdictions and comply with the data protection requirements of the jurisdiction from which the information originates.

- **Policies & Procedures.** A company's policies and procedures can establish the framework necessary to protect sensitive employee information. Employers may also require proper usage of company resources and should include such requirements in their employment

[71] *See* RESTATEMENT (SECOND) OF AGENCY § 405 (for discussion of liability between agent and principal).

handbooks or labor manuals as internal policy. Policies can specify retention periods, proper methods for destruction of personal data, and redaction and copying policies. In appropriate circumstances, a company's handbook and policy statements can also serve to notify employees of how their information will be handled, where it may be transmitted, and may provide a mechanism to address any employee concerns.

- **Physical & Technological Safeguards.** Outsourcing contracts and employment policies can specify appropriate physical technological safeguards for personal data to ensure that the information is transmitted, retained and destroyed in a manner that prevents unauthorized use or disclosure. These safeguards can include a prohibition on bringing any items that could be used to store personal data in or out of a restricted area. Employers also can limit access to those individuals with a "need to know." Tracking numbers, encryption and other technologies that prevent copying also may be employed.

- **Investigate Third Party Providers, Employees & Individuals Who Will Have Access to Personal Information.** To the extent a company intends to use a third-party provider to house information off-shore, an employer should scrupulously investigate the foreign company it selects to handle the personal information of employees, both in terms of its professional integrity and competence. The thoroughness of the investigation should correspond to the sensitivity and the volume of the information, and may in certain circumstances require the assistance of an investigator or other professional. An investigation may include conducting a background check of the company, obtaining and contacting references, verifying the company's past performance and reputation in the industry, requiring the company to complete an information security questionnaire, and evaluating any claims leveled against the company. An investigation may also include interviewing, choosing, and investigating the individuals who are charged with performing the work. It may require that the company or employee is professionally credentialed. A company should confirm that the foreign company or individual is familiar with privacy requirements of the jurisdiction from which the information originates.

- **Monitor & Audit.** Periodic audits will help verify that the policies, procedures, and safeguards initially put into place are actually followed and accomplish their intended purposes. The audits also will provide a mechanism to reassess and modify policies in light of developing practices, law, and technology.

- **Obtain Advice on Rights & Remedies Available in the Jurisdiction.** An informed legal opinion in the applicable jurisdiction is important to determine the remedies that are available for a security breach involving confidential information. When crafting appropriate safeguards, a legal opinion also will be important to determine the enforceability of the desired safeguards. A company should consider not only the substantive laws of the jurisdiction concerning confidentiality and privacy, but also other procedural and substantive rules that can impact the ability to maintain privacy. For example, a company that enters a contract with a third-party provider, employee, or contractor in another country will have to obtain an opinion on the enforceability of the agreement and its provisions.[72] If a choice-of-

[72] For a discussion on how choice of laws issues in contracts are being handled in China, see Mo Zhang, *Choice of Law in Contracts: A Chinese Approach*, 26 N.W. J. INT'L L. & BUS. 312, 312–27 (2006) (citing the 1985 Foreign Economic Contract Law, Article 5 (permitting choice of law specification in a contract to settle the an issue in the contract)); *see also, e.g.*, *Black Sea Steamship UL Lastochkina Odessa, USSR v. Union of India* (AIR 1976 AP 103) (finding it "perfectly open to the court to consider the balance of convenience, and interests of justice and like circumstances when it decides the question of jurisdiction of a court in the light of a clause in the agreement

law provision is not effective in a particular jurisdiction, then its inclusion in a contract will be useless. An opinion also will be needed regarding the likely interpretation of any agreement. Advice on contending with the practical problems of a country's particular legal system also will be of great benefit. Once information is transferred to a jurisdiction, an opinion on the ability to gain access to that information in that jurisdiction likely will be necessary to determine the effectiveness of attempted safeguards. As merely one example, certain assessments or reviews of employees may be considered libel or slander[73] in certain countries and could prompt attempts to gain information through the legal process.

Although the transfer of private information between jurisdictions likely will cause some uncertainty in terms of conflicting laws, a company can and should consider a wide range of innovative options to meet the privacy challenges facing an increasingly multinational workforce.

§ 4 PRACTICAL GUIDELINES FOR EMPLOYERS

§ 4.1 SAFEGUARDING EMPLOYEE PERSONNEL DATA FROM THEFT

With the latest and greatest technological advancement comes the risk for potential security breaches. Such security breaches can result in damaging publicity, significant out-of-pocket expenses and undercut employee and customer loyalty. Employers should consider the six-pronged approach outlined below protecting the organization's personnel information from unauthorized access and to mitigate damage to employees when a security breach does occur.

- **Establish a Data Protection/Privacy Policy.** The data protection/privacy policy should embody all aspects of the employer's efforts to reduce the risk of unauthorized access to personnel data. The policy should accomplish at least the following:

  - Identify the circumstances in which sensitive data may be collected from job applicants and employees, the types of data to be collected and how the employer may use and disclose the data.

  - Strictly limit the collection, use and disclosure of sensitive data to the minimum necessary for the intended purpose.

  - Eliminate all unnecessary collection, uses and disclosures of personal information.

  - Detail how the employer will safeguard sensitive personal data.

  - Explain how employees can identify and report possible security breaches.

  - Establish procedures for responding to security breaches. This should include building an incident response team, to include information technology (IT) personnel, human resources professionals, business unit leaders, in-house or outside counsel and public relations specialists. Team members should be assigned specific roles and responsibilities in responding to a security incident.

---

between parties choosing one of several courts or forums which were available to them"); INDIA CIV. PROC. CODE § 13 (foreign judgments are conclusive absent certain exceptions), 15 & 44A (decrees from reciprocating territories are enforceable).

[73] *See, e.g.*, Tariq Engineer & Jessica E. Vascellaro, *Google Faces Defamation Lawsuit in India*, WALL ST. J., Aug. 15, 2008.

- Sanction employees who violate the data protection policy.

- Describe how the employer will mitigate potential damages to affected individuals when a security breach does occur.

- **Control Access to Sensitive Data.** Access to sensitive employee data should be restricted, controlled and monitored. One approach to these tasks entails the following steps:

  - Identify the categories of employees who may access sensitive data.

  - Identify the categories of sensitive data that may be used and disclosed by each employee granted access.

  - Restrict access to the most sensitive data to employees with a track record for trustworthiness or who have been subjected to a background check.

  - Periodically review access rights and revise access lists as may be necessary to reflect any change in employers' job responsibilities.

  - Upon terminating an employee with authorized access to sensitive data, promptly change all passwords and security codes available to the terminated employee and require the immediate return of computer disks, compacts disks, keys, laptop computer and other mobile devices; after terminating an employee with authorized access to sensitive data, strip the employee's computer of sensitive data before reissuing the computer to another employee.

  - Bar temporary, outsourced and vendor employees from sensitive data except when absolutely necessary. When access is necessary, the employer should conduct a background check or ensure that the temp agency, outsourcer or vendor has done so. The employer also should monitor these employees' use and disclosure of sensitive data to the maximum extent feasible. Consider obtaining confidentiality agreements from the employees of vendors.

    Before sharing sensitive data with an outsourcer, conduct due diligence concerning the outsourcer's "*bona fides*," including its security policies and procedures. In addition, negotiate a written agreement with the outsourcer that addresses the following terms:

    - the outsourcer's permitted uses and disclosures of the information;

    - the administrative, physical and technical safeguards the outsourcer must implement;

    - prompt notice to the employer in the event of a security breach;

    - the outsourcer's obligation to assist in mitigating damages;

    - indemnification to the employer for any damages caused by the outsourcer's security breach;

    - the employer's right to audit the third party's security controls;

- restrictions on the outsourcer's use of subcontractor's or agents and/or a requirement that the outsourcer obtain the written agreement of any outsourcer or agent to provide similar safeguards;
- choice of law and choice of forum;
- amendment of the agreement in the event of any change in controlling law; and
- any other matter that must be addressed in the agreement for legal compliance purposes.

- **Technical and Physical Safeguards.** The employer's information technology department should put in place an array of security measures for electronic data, including the following:
  - assignment of a unique identifier to each network user to permit monitoring of user activity;
  - password protection and, where appropriate, encryption for all files containing sensitive data;
  - use of complex passwords (with at least eight characters, at least one capitalized letter and at least one number) that are changed regularly;
  - installation and regular updating of firewalls and antivirus software;
  - prompt implementation of patches for security holes;
  - lockdown of workstations capable of accessing sensitive data during periods of inactivity;
  - logging access to files containing sensitive data and monitoring any outward transfer or duplication of those files;
  - use of hardware and software to record and examine activity on information systems;
  - prohibiting the downloading of sensitive data to laptops, mobile devices and portable storage media except when necessary to perform job responsibilities and when feasible if the downloaded information will be encrypted; and
  - destruction of electronic files in a manner that ensures that they cannot be retrieved.

  Implementing the following procedures for securing sensitive data in paper format remains essential as well:

  - paper documents containing sensitive data should be stored only in areas with employees authorized to access those documents;
  - employees with access should lock all file drawers, cabinets and offices containing sensitive paper records when unattended;
  - computer printers, scanners and fax machines for employees who use and disclose sensitive data as part of their job functions should be maintained in a controlled area;

- the memory dial program on the secure fax machine should be regularly monitored for outdated and incorrect numbers; and

- sensitive data in paper form should be shredded either internally or by a bonded company.

- **Training.** Like any workplace policy, a data protection/privacy policy has value only if employees understand it and abide by it. Consequently, central to the policy's success will be a program to train employees—especially those with access to sensitive data—to reduce security risks and vulnerabilities, to detect possible security breaches and to respond to a suspected security breach. The training should encompass at least the following:

  - "password etiquette," *i.e.*, selecting unpredictable passwords and avoiding disclosure of passwords to coworkers and outsiders;

  - teaching employees proper procedures for storing, printing, transmitting and destroying documents containing sensitive data; and

  - training employees to recognize and report a suspected security breach.

- **Responding to a Security Breach.** If the employer has established an incident response team, the team should be prepared to investigate, mitigate and remediate the breach immediately. The team will also need to address potential employee, customer and/or media relations issues and oversee compliance with all applicable data breach notification requirements.

- **Notice of a Security Breach.** All states, the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands have implemented security breach notification laws. (See discussion at **§ 2.2(c)(iii)**.) Even when not legally required to provide notice, employers evaluate whether doing so is appropriate from an employee relations perspective. Prompt notice provides employees with an opportunity to protect themselves before identity thieves have the opportunity to misuse the personal data stolen from an employer. In addition, employees who act promptly most likely will spend less time (including time at work) trying to restore their credit. Providing prompt notice as well as additional assistance also is a way for employers to demonstrate concern for employee welfare and generate employee loyalty.

  While breach notification laws may impose additional requirements, some recommendations concerning the content of such a notice include the following:

  - Briefly describe the circumstances that caused the security breach, including the date that the breach was discovered.

  - Specify the categories of employee personal information (*i.e.*, Social Security number, account numbers, health information, etc.) that were, or might have been, subject to unauthorized access.

  - Describe the steps taken to mitigate the security breach and the steps that will be taken to prevent a recurrence.

  - Describe any offer of identity protection services, such as credit monitoring or fraud resolution services.

- Encourage employees to act promptly to protect their identity by closing potentially affected accounts and warning creditors of potentially fraudulent activity.

- Advise employees to consider exercising their rights under federal law for potential victims and victims of identity theft, including the right to place a fraud alert and an extended fraud alert with the nationwide credit bureaus, the right to block consumer reporting agencies from reporting information that results from fraud, and the right to obtain from businesses information concerning accounts or transactions resulting from fraud.

- Suggest that the employee visit the FTC's website to obtain additional resources for victims of identity theft, such as the FTC's publication, "When bad things happen to your good name."

- Provide employees with information for obtaining a free annual credit report from each of the three national credit bureaus, and encourage them to monitor their credit reports.

- Several states mandate specific additional content in a security breach notification. Consult with counsel regarding these requirements.

- When notice to employees is legally required, the employer also may be required to notify government agencies, the national credit bureaus, and/or the media. Employers should consult counsel to determine whether such notices are required.

Employers should maintain a copy of each notice mailed to employees, or of a template notice, and a mailing list in the event the employee ever files a lawsuit alleging that the employer is responsible for losses from the identity theft. Employers should also maintain documents evidencing a decision not to provide notice to potentially affected individuals.

§ 4.2 TRANSBORDER DATA TRANSFERS

The European Union is undergoing a major reform of its data privacy laws following the invalidation of the Safe Harbor Framework and the passage of the General Data Protection Regulation (GDPR). New guidance from E.U. data protection authorities is being issued as the data privacy law in Europe continues to evolve. Multinational employers should continue to monitor these developments and watch for additional guidance. Additional recommendations include:

- U.S.-based multinational employers should monitor the status of the Privacy Shield and consider implementing alternative methods for lawfully transferring the personal data of E.U. employees to the United States.

- U.S. multinationals should take advantage of the two-year grace period to come into compliance with the GDPR. To comply with the GDPR, virtually all U.S.-based multinational employers likely will need to update at least some of their existing policies and procedures, and re-align some of their practices, for handling the personal data of employees of their E.U. subsidiaries.

- The invalidation of the Safe Harbor framework has had a domino effect in other jurisdictions that had similar agreements with the United States. U.S. multinational employers should review the jurisdictions in which they operate to confirm that no other transborder data transfers were affected by the invalidation of the Safe Harbor framework.

§ 4.6(a) *Implementing a Privacy Shield Compliance Program for Transfers of HR Data*

Satisfying the formal requirements for self-certification under the new Privacy Shield will be relatively straightforward, but achieving meaningful compliance that mitigates enforcement risk will be far more complicated, and enforcement risk, particularly for transfers of HR data, has increased materially. To begin with, virtually all enforcement will take place in the European Union, *not* the United States. Second, E.U. DPAs, particularly in countries like France, Germany and Spain, appear to be primed to flex their enforcement muscle. Third, while E.U. employees may not grasp all the nuances of the debate over the Safe Harbor, they and their works council or trade union have become generally leery of large-scale transfers of HR data to the United States. As a result, they may initiate complaints, especially if they sense that the U.S. parent corporation is not taking data protection seriously.

To demonstrate its commitment to compliance to its E.U. employees (and their representatives) and, if needed, to regulators, the U.S. parent corporation should consider taking the following steps:

1. **Confirm that E.U. subsidiaries comply with local requirements for cross-border data transfers to the United States.** The Privacy Shield framework document emphasizes that the "Privacy Shield Principles are relevant only when [HR data is] transferred or accessed" and that collection and processing of HR data "prior to transfer will have been subject to the national laws of the EU country where it was collected, and any conditions for or restrictions on its transfer according to those laws will have to be respected."[74] As a practical matter, this requirement to comply with local laws means that E.U. subsidiaries must take the following steps before transferring their employees' personal data to the United States pursuant to the Privacy Shield: (1) provide their employees with notice of data processing, including transfer to the United States; (2) consider local law restrictions on cross-border data transfers, particularly on transfers of sensitive personal data, such as employees' health information; (3) confer with works councils or trade unions, if any and if legally required, concerning data transfers to the United States; and (4) depending on the country, register with or notify the local DPA of data processing, including cross-border data transfers.

   In a world where technology permits a small or medium-sized U.S. business to be a multinational employer, many E.U. subsidiaries of organizations that will certify to the Privacy Shield are only small sales offices or factories with no locally-assigned HR professional or legal counsel. As a result, these subsidiaries likely will address compliance with local data protection laws for the first time when the U.S. parent corporation decides to transfer E.U. employees' personal data to the United States.

2. **Establish policies and procedures to implement the privacy shield privacy principles**. While the HR privacy policy submitted to the Commerce Department will contain the high-level principles that should guide the handling of E.U. employees' personal data transferred to the United States, that policy typically will not instruct U.S.-based HR professionals, payroll personnel, managers and others on exactly what it is they need to be doing to achieve compliance. For example, the Privacy Shield framework document requires certifying organizations to satisfy the Security Principle by "tak[ing] reasonable and appropriate measures to protect [transferred personal data] from loss, misuse and unauthorized access, disclosure, alteration and destruction."[75] However, that document identifies *no* specific measures to be taken. Because there is a similar lack of detail for most of the other Principles,

[74] Supplemental Principles, § III.9.a.i, *available at* https://www.privacyshield.gov/EU-US-Framework.

[75] Principles, § II.4.a.

certifying organizations will need to develop detailed policies and procedures to implement the Principles. Some of those policies and procedures include:

a. *Notice & Choice Principles:* U.S.-multinational employers typically will transfer E.U. employees' personal data to the United States to store it in a centralized HR information system ("HRIS") that facilitates global workforce management. Given this purpose, the HR privacy policy likely will inform the E.U. workforce only about the use and disclosure of their personal data for HR administration purposes. If the U.S. parent subsequently were to use transferred personal data for other purposes, such as to market the company's products to the E.U. workforce or to support a global charitable campaign, it would be required to give E.U. employees the opportunity to opt out from the previously undisclosed use. According to the Privacy Shield framework document, such "choices must not be used to restrict employment opportunities or take any punitive action against such employee."[76] In other words, E.U. employees cannot be confronted with a choice between consenting to the new use or losing their job. As a benefit to employers, the Privacy Shield specifically excludes from the Notice and Choice Principles processing E.U. employees' personal data for "promotions, appointments or other similar employment decisions." This exclusion applies only "[t]o the extent and for the period necessary to avoid prejudicing" the decision-making process.[77] This exclusion should help to avoid a situation where notice disrupts the employment decision-making process.

   To handle transferred data in compliance with the Notice and Choice Principles, the certifying organization should consider implementing several policies and practices. By way of illustration, it should specifically identify the categories of employees authorized to access E.U. employees' personal data; the categories of data that can be accessed; the permissible purposes for access, use and disclosure; and the steps to be taken before using such data for a purpose not previously disclosed in the HR privacy policy or otherwise.

b. *Accountability for Onward Transfer Principle:* Under the Accountability for Onward Transfer Principle, certifying organizations must require, by written agreement, that third parties who receive transferred personal data provide the same level of protection for that data as required by the Privacy Shield. The U.S. parent corporation must enter into these "onward transfer agreements" with both agents, such as HR service providers and non-agents that will use transferred personal data for their own purposes. Organizations that certified to the Privacy Shield within 60 days of its effective date (*i.e.*, September 10, 2016) had 9 months from the date listed on the Privacy Shield List to bring contracts with third parties into conformance with this Principle.

   The Privacy Shield establishes an important exception from the requirements described above for cross-border data transfers within a corporate group. The U.S. parent corporation can make such transfers without an "onward transfer agreement" provided that "other instruments, such as EU Binding Corporate Rules [BCRs] *or other intra-group instruments (e.g., compliance and control programs*), ensuring the continuity of protection of personal information under the Privacy Shield Principles" have been implemented.[78] The italicized phrase gives U.S. parent corporations greater flexibility

[76] Supplemental Principles, § III.9.b.i.

[77] Supplemental Principles, § III.9.b.iv.

[78] Supplemental Principles, § III.10.b.i (emphasis added).

because it allows them to forego not only onward transfer agreements but also the potentially onerous process of implementing BCRs when those organizations need to share E.U. employees' personal data with non-U.S. and non-E.U. affiliates, for example, when an HR director for Europe, the Middle East and Africa ("EMEA") resides in the United Arab Emirates.

c. *Security Principle:* To satisfy this Principle, the U.S. organization will need to implement specific measures, such as access controls, restrictions on storage of E.U. personal data on portable storage media, safeguards for paper records containing E.U. personal data, and secure methods of document disposal. The organization may be able to leverage for this purpose policies and practices used to safeguard other types of sensitive employee data, such as Social Security numbers and protected health information subject to the Health Insurance Portability and Accountability Act (HIPAA).

d. *Access Principle:* Under the Access Principle, individuals have the right to access their personal data, to correct personal data that is inaccurate and to delete personal data that the U.S. organization processes in violation of the Principles. However, the detailed procedures established by the Privacy Shield framework for implementing these rights have limited applicability to HR data transferred in the context of the employment relationship. The Privacy Shield dictates that "employers in the European Union must comply with local regulations and ensure that European Union employees have access to such information as is required by law in their home countries, *regardless of the location of data processing and storage*."[79] The Privacy Shield also mandates, in light of E.U. employees' rights under local law, that the U.S. parent corporation "cooperate in providing such access either directly or through the EU employer."[80] Consequently, certifying organizations will need to implement policies and procedures to facilitate a coordinated response to requests by E.U. employees to exercise their rights to access, amend and delete their personal data.

3. **Establish an annual verification process.** The Privacy Shield requires that certifying organizations recertify annually, and that before recertification, they verify on-going compliance with the Principles. The verification can be conducted as a self-assessment or by an outside entity. In either case, the certifying organization must verify that the attestations in its self-certification and assertions in its HR privacy policy are true and that "privacy practices have been implemented as represented and in accordance with the Privacy Shield Principles."[81] To meet those standards, organizations that choose to conduct a self-assessment must verify that:

a. the HR privacy policy is "accurate, comprehensive, prominently displayed, completely implemented and accessible;"

b. the HR "privacy policy conforms to the Privacy Shield Principles;"

c. individuals are informed how to submit complaints, both internally and to the relevant E.U. data protection authority;

d. employees with access to transferred personal data have received training and will be

[79] Supplemental Principles, § III.9.c.i (emphasis added).

[80] Supplemental Principles, § III.9.c.i (emphasis added).

[81] Supplemental Principles, § III.7.a.

disciplined for policy violations; and

e. the organization conducts periodic compliance reviews.[82]

The verification must be signed by an authorized corporate representative and must be produced upon request to employees, or in the context of an investigation or complaint proceeding.

4. **Be prepared to resolve complaints in the European Union.** U.S. organizations that certify to the Privacy Shield to transfer HR data are required to agree to cooperate with investigations by, and abide by the advice of, E.U. data protection authorities. Notwithstanding this certification by the U.S. parent corporation, the Privacy Shield framework document emphasizes that even after HR data is transferred, "primary responsibility for that data vis-à-vis the employee remains with the organization in the EU."[83] Consequently, the framework document provides that E.U. employees who are not satisfied with the internal resolution of their data protection complaints "should be directed to the state or national data protection or labor authority in the jurisdiction where the employees work" even if the U.S. parent corporation is responsible for the alleged violation.[84]

   To fulfill its representation in the self-certification form, the U.S. parent corporation would be required to participate in the complaint proceeding in the European Union with its E.U. subsidiary. Significantly, this proceeding will be governed by the relevant E.U. Member State's law and not by the Principles or U.S. law. In addition, the U.S. parent corporation will be required to abide by the advice of the DPA, which could include an order to implement remedial measures and/or to compensate the employee.

[82] Supplemental Principles, § III.7.c.

[83] Supplemental Principles, § III.9.d.i.

[84] Supplemental Principles, § III.9.d.i.

