Proskauer

What Employers Need to Know about Europe's New General Data Protection Regulation

For more information, please contact:

Erika C. Collins
Partner
+1.212.969.3555
ecollins@proskauer

Michelle A. Gyves
Associate
+1.212.969.3554
mgyves@proskauer

Arielle E. Kobetz
Associate
+1.212.969.3304
akobetz@proskauer

Proskauer

What Employers Need to Know about Europe's New General Data Protection Regulation

A. Summary

On April 14, 2016, the European Parliament approved the General Data Protection Regulation ("GDPR" or the "Regulation"), a new regulation that will replace the European Union's ("EU") current data privacy standard.[1] As a regulation, the GDPR will impose a more uniform data protection regime across the Member States and makes more clear the extent of its jurisdictional reach than did its predecessor. Though the GDPR is not specific to the employment context, it is clear that the "processing" of employee data falls within the scope of its protection. This paper provides a broad overview of the ways in which the GDPR will change data protection regulations across the EU, focusing on employee data and how it is treated differently from consumer data. This paper also highlights key areas of change from the current state of the law and suggests proactive steps an employer may take to better prepare for May 25, 2018,

Companies in the U.S. and around the world should have an important date circled on their calendars:

May 25, 2018

the date on which the GDPR will start to apply.

B. Introduction

In 1995, the EU passed the European Union Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, more commonly referred to as "the Directive." *See* Commission Directive 95/46/EC [hereinafter Directive]. The Directive created a broad set of data protection standards and mandated that all Member States transpose into national laws its provisions and principles. *Id.* Established under the Directive, the Article 29 Working Party is an independent European advisory body that works to promote the application of the Directive and ensure its primary objectives are met. *Id.* at art. 29. Among those objectives is the protection of "the fundamental rights and freedoms of natural persons and, in particular, their right to privacy with respect to the processing of data," which is to be balanced against the facilitation of the "free flow of personal data" across Member States. *Id.* at art. 1(1), (2). To realize this goal, the Directive prohibits all processing of data unless the processing is fair, lawful, and "for specified, explicit, and legitimate purposes." *Id.* at art. 6(1)(a), (b). The Directive further prohibits the transfer of data to any country outside of the EU unless that country has an "adequate" level of protection as determined by the EU Commission. *Id.* at art. 25.

---

[1] *See* Position of the Council at first reading with a view to the adoption of a Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), COD (2012) 0011 (Apr. 6, 2016) [hereinafter GDPR].

Importantly, the Directive serves only as a framework for data privacy laws, as each Member State was required to enact its own legislation in order to make the Directive law within that country. *Id.* at art. 4(1), art. 32(1). As such, it has become increasingly difficult for businesses to keep up with all the varying requirements. In particular, the Directive's jurisdictional scope was uncertain and companies based outside of the EU who wanted to target EU customers were left unsure of their responsibilities under the Directive, and could at least make the argument that the Directive did not even apply.

Furthermore, since the Directive's implementation more than two decades ago, technology and the use of the internet have rapidly evolved, leading businesses to expand their operations and use of personal data. By repealing and replacing the Directive with the GDPR, the EU is recognizing and responding to such changes. Moreover, as a regulation instead of a directive, the GDPR will harmonize data protection regulations across the EU and eliminate much confusion in attempting to determine how each Member State addresses each principle. The GDPR also will replace the current Article 29 Working Party with the European Data Protection Board (EDPB), comprised of the EDP Supervisor and senior representatives of the national data protection authorities. As discussed in more detail below, however, the GDPR acts a floor in that Member States may still implement their own regulations, particularly in the employment context. *See* GDPR recital (10), (155). Moreover, while it does not explicitly apply to employee data, it is apparent that employees' personal data is of the kind the GDPR aims to protect. Accordingly, employers must be aware of the changes stemming from the GDPR, as well as any additional regulations governing each Member State in which it deals with the transferring and/or processing of employees' personal data.

C. The GDPR

In April of 2016, the European Parliament approved the final draft of the GDPR, which officially will repeal and replace the Directive when it starts to apply on May 25, 2018. *See* GDPR art. 94. While certain provisions of the GDPR remain unchanged from, or are very similar to, the provisions of the Directive, there also are some critical differences, as discussed in more detail below. Importantly, unlike the Directive, the GDPR is directly applicable to each Member State and therefore does not require each state to enact its own legislation, providing a sense of predictability and stability to those entities subject to the GDPR. Nevertheless, as noted above, each Member State may still implement its own regulations so employers must continue to remain vigilant of Member State-specific, and potentially conflicting, principles with respect to processing employees' personal data.

As an initial matter, the definitions of data "controller," data "processor," and "processing" are unchanged from the Directive. A data controller is defined as the person or entity that "determines the purposes and means of the processing of personal data[…]", *id.* at art. 4(7), which generally will include employers processing the data of their employees. A data processor is the person or entity that "processes personal data on behalf of" a controller (such as an employer). *Id.* at art. 4(7), (8). Processing involves "any operation or set of operations which is performed on personal data," whether or not by automated means. *Id.* at art. 4(2). The GDPR retains the Directive's "all means reasonably likely to be used to identify" test to determine whether the Regulation applies to a company's processing activities. *Id.* at recital (26). In other words, the GDPR applies to all data from which an employee is identified or identifiable (by anyone), whether directly or indirectly. *Id.*

Of note, the GDPR incorporates a concept known as "data protection by design," wherein employers must implement appropriate safeguards "both at the time of the determination of the means for processing and at the time of the processing itself." *Id.* at art. 25(1). This places onerous accountability obligations on an employer to demonstrate its compliance with the GDPR, including, *e.g.*, the adoption and implementation of internal policies and measures, and the maintenance of records of processing activities under its responsibility. *See id.* at recitals (78)-(84). Accordingly, and in light of the principles noted below, an employer should carefully outline its procedures going forward, and document any and all steps it takes with respect to processing of employees' personal data. This is particularly important as such measures will be considered as mitigating factors if and when penalties are to be imposed. *Id.* at art. 83(2).

a. Data Processing Standards

How should employers process their employees' personal data? The standards for processing under the GDPR are very similar to those under the Directive, as Article 5 of the GDPR upholds and expands upon the principles outlined in Article 6 of the Directive.

- **Lawfulness, Fairness, and Transparency:** employees' personal data must be processed lawfully, fairly and in a transparent manner in relation to the employee. This requires that employers provide all information to its employees in clear, intelligible, and plain language in an easily accessible form. *See id.* at art 5(1)(a), recital (60);
- **Purpose Limitation:** personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes";
- **Data Minimisation:** personal data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed";
- **Accuracy:** personal data must be "accurate and, where necessary, kept up to date" and "every reasonable step" must be taken to ensure that "inaccurate" data is "erased or rectified without delay";
- **Storage Limitation:** personal data must be "kept in a form which permits identification of [employees] for no longer than is necessary for the purposes for which the personal data are processed…"; and
- **Integrity and Confidentiality:** data must be processed "in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures."

Id. at art. 5(1)(a)-(f).

Referring back to the notion of "data protection by design," employers also must take into account "the state of the art, the costs of implementation and the nature, scope, context and purposes of processing" when implementing appropriate measures to ensure a level of security "appropriate to the risk." *Id.* at art. 32(1). Unlike the Directive, the GDPR provides specific suggestions as to what tools a company may use to demonstrate its compliance with this principle, including: (1) the pseudonymisation and encryption of personal data; (2) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (3) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or

technical incident; and (4) a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing. *Id.* at art. 32(1)(a)-(d). Recital 81 similarly requires employers to engage only those processors "providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organizational measures which will meet the requirements of this Regulation, including for the security of processing." Employers may – and, pursuant to Article 5(2), must – demonstrate compliance with these obligations by adhering to an approved code of conduct or certification mechanism, which are discussed further in subsection (f) below. *Id.* at recital (81).

The GDPR's definition of "lawful processing" is largely unchanged from that of the Directive. Like the Directive, the GDPR provides that processing is lawful in the employment context where it is (1) necessary for an employer to perform its contractual obligations vis-à-vis an employee (*e.g.*, processing an employee's salary data); (2) necessary for an employer to comply with a legal obligation (*e.g.*, processing an employee's data for the purpose of calculating the withholding tax); (3) necessary to protect the employee's vital interests where the employee is incapable of giving consent (*e.g.*, an employer may compile medical data regarding the employee to protect the employee against particular hazards at the workplace); or (5) necessary for the purposes of legitimate interests (*e.g.*, where an employer transmits employees' personal data within its corporate structure for internal administrative purposes). *Id.* at art. 6(1)(b)-(f), recitals (47)-(48). The GDPR also recognizes that processing is lawful where the controller obtains the data subject's consent; however, as discussed in subsection (c) below, the GDPR sets out a more robust definition of consent.

With respect to "further processing," as defined in Article 6(4), where such processing is not based on the data subject's consent, the GDPR provides the following as a list of factors to consider when determining whether further processing would be "compatible" with the original purpose for which the data was processed: (1) any link between the original and proposed new purposes; (2) context in which data have been collected (in particular, the relationship between the employee and the employer); (3) the nature of the data (whether it is sensitive or criminal data); (4) possible consequences of the proposed processing; and (5) the existence of safeguards, including encryption and pseudonymisation. *Id.* at recital (50).

b. Consent

As noted above, processing is lawful where a data subject has consented to such processing. Article 4 defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." *Id.* at art. 4(11).[2] Affirmative action signaling consent may include (1) ticking a box on a website; (2) "choosing technical settings for information society services"; or (3) "another statement or conduct" that clearly indicates consent. *Id.* at recital (32). This is more restrictive than the Directive, which allows data controllers to rely on implicit and "opt out" consent in some cases. *See* Directive, art. 2(h). Like the Directive,

[2] The GDPR specifically recognizes that children require greater protection with respect to giving consent. It sets the age of consent at sixteen (16) years old; however, Member States may set a lower age, not below thirteen (13) years. *Id.* at art. 8(1). Where an employee cannot give consent based on his or her age, an employer must make "reasonable efforts" to verify that a parent or guardian provided the appropriate consent. *Id.* at art 8(2).

"silence, pre-ticked boxes or inactivity" remain inadequate indicators of consent. GDPR, recital (32). Moreover, consent must be specific to each data processing operation. *Id.* For example, if consent is provided in a written document, it must be "clearly distinguishable" from any other matters. *Id.* at art. 7(2). A data controller bears the burden of demonstrating that it obtained the data subject's lawful consent. *Id.* at art. 7(1).

Notably, consent continues to be viewed skeptically by the EU Commission and so employers should strive to fit the reason for processing under another derogation. Employers are advised to avoid consent whenever possible and instead consider other permissible purposes for which it may collect and process employee data. When providing notice to its employees regarding the data it intends to collect, an employer should be inclusive but also ensure that it is not collecting data that it does not need. Given society's growing sensitivity to personal data breaches and hacks, it is more important than ever to ensure the reasons for collecting an employee's personal data fits into one of the GDPR's derogations – particularly since employees are far less likely to give consent and because employees may withdraw consent at any time.

Employers are advised to avoid consent whenever possible and instead consider other permissible purposes for which it may collect and process employee data.

Finally, the GDPR affords employees the right to withdraw consent at any time and "it shall be as easy to withdraw consent as to give it." *Id.* at art. 7(3). An employer must inform employees of the right to withdraw before consent is given, so the right to withdraw consent should be embedded in the notice provided to employees. *Id*. Once consent is withdrawn, employees have the right to have their personal data erased and no longer used for processing. *Id.* at art. 17(1)(b). As discussed further in subsection (h) below, this right to erasure, in addition to other new individual rights afforded by the GDPR, places a significant burden on companies to develop the capabilities necessary to comply with employees' requests and ensure GDPR-compliant data transfers.

The inequality inherent to an employer-employee relationship raises issues with respect to obtaining proper consent, as an employee may be viewed as having not freely consented to the employer's processing of his or her personal data. As noted above, consent has always been viewed skeptically by the EU Commissioner in the context of the employment relationship. It is not always easy to determine whether an employer has given such unambiguous consent. For example, does the conclusion of a written employment agreement that includes consent to process data in the text constitute unambiguous consent? Probably not; especially in light of the fact that at-will employment is not recognized in the EU and thus an employer may not tie an employee's unambiguous consent to process data to that employee being hired or remaining employed, as such consent has not been given freely. Moreover, an employer-employee relationship can be a volatile one and employees may ultimately withdraw consent based on workplace morale. In practice, employers should use a "belt and suspenders" approach to protect against liability, only using consent as a fall back provision and documenting how its processing operations also falls under one of the other derogations.

c. Notices

The GDPR contains more expansive requirements regarding the information that an employer must provide to a data subject regarding the collection and processing of his or her personal data.

Under the Directive, data controllers were explicitly required to disclose only "the identity of the controller and of his representative, if any; the purposes of the processing for which the data are intended; [and] any further information . . . in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing." Directive, art. 10. Examples of such further information include "the recipients or categories of recipients of the data, whether [providing the data is] obligatory or voluntary, as well as the possible consequences of failure to reply, [and] the existence of the right of access to and the right to rectify the data." *Id.* Similar requirements applied for data collected from sources other than the data subject. *Id.* at art. 11.

The GDPR, by contrast, provides a more explicit (and more expansive) list of information that must be provided to a data subject in connection with the collection of his or her personal data. Specifically, a controller (such as an employer) is required to provide:

- The identity and contact information of the controller and its representative (where applicable);
- The contact information of the data protection officer (if applicable);
- The purposes of the processing and the legal basis for the processing;
- Where processing is to further a legitimate interest of the controller (employer), an explanation of the legitimate interest(s) being pursued;
- The recipients or categories of recipients;
- If applicable, an indication that the controller (employer) intends to transfer the personal data to a third country, an indication of whether such country is the subject of an adequacy decision, and reference to the appropriate safeguards;
- The period for which the data will be stored;
- The rights to access, rectification, erasure, restriction, objection, and portability;
- Where processing is based on consent, the right to withdraw consent;
- The right to lodge a complaint with a supervisory authority;
- Whether the provision of data is required (by statute or contract), whether the data subject is obliged to provide the data, and the consequences of not providing the data; and
- The existence (if applicable) of automated decision making, including profiling, and information about the logic involved and the significance and consequences of the processing for the data subject.

GDPR art. 13. When personal data is collected from a source other than the data subject, the data controller also must advise the data subject of the categories of personal data concerned and the source of the data, including whether it came from any publicly available sources. *Id.* at art. 14.

Employers should review their privacy notices, policies, and other documentation and communications to comply with these expanded disclosure obligations.

d. Processing Sensitive Data

Like the Directive, the GDPR requires explicit consent for processing "special categories" of personal data. *Id.* at art. 9(2)(a).[3] The Regulation expands the Directive's definition of special categories of data to include: (1) revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership; and (2) processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a person's sex life or sexual orientation. *Id.* at art. 9(1).

> Employers should review their privacy notices, policies, and other documentation and communications.

The GDPR recognizes certain derogations that allow for the processing of special categories of data absent explicit consent including, for example, where the processing is necessary for "the assessment of the working capacity of the employee." *Id.* at art. 9(2)(h), recital (52).

Many employers process at least some sensitive data almost unwittingly as this has become part of their "standard procedure." Some may wish to conduct drug testing in the workplace or gather genetic testing data to assess an employee's working capacity and for other purposes, such as administering employee wellness programs. While the GDPR allows for the processing of such data absent employee consent in some situations, employers must proceed with caution when processing health and medical data to ensure they do not cross the line of invasion of privacy and disrupt employee morale. Doing so would not only make the employer vulnerable to liability, but also other employees in the company may become nervous about the reasons for and means by which the employer processes their data, and subsequently withdraw consent and/or demand erasure of their personal data, as discussed below. Further, as more and more employees abandon the traditional work-place setting in favor of working from home or other non-traditional settings, the line between working time and personal time becomes increasingly blurry. Employers wishing to engage in surveillance and monitoring of its employees at the workplace should proceed with caution, as the Commission likely will closely scrutinize an employer's activities to be sure it does not constitute an invasion of employees' privacy – whether or not such invasion is intentional. Where possible, employers should process sensitive data only in very limited cases and, again, use employee consent only as a backup plan. In practice, employers should offer a separate consent form to its employees – a document separate from any employment agreement that explicitly states the reasons for which the employer processes the employee's sensitive data – so that the employee's signature indicates unambiguous consent.

e. Data Protection Officer

Article 37 of the GDPR imposes a new requirement on both controllers and those vendors with whom they contract to process personal data: the appointment of a data protection officer ("DPO"). This obligation applies to (1) public authorities; (2) where the core activities of the controller or processor involve "regular and systematic monitoring of data subjects on a large scale"; and (3) where the entity conducts large scale processing of special categories of personal data. *Id.* at art. 37(1)(a)-(c). While the definitions of "core activities" and "large scale" are not clear under the GDPR the Article 29 Working Party recently

[3] The GDPR allows individual Member States to enact laws that restrict the processing of some categories of data even if the data subject explicitly consents. *Id.* at art. 6(2).

issued its first set of guidance with respect to certain provisions of the GDPR, including the DPO. According to the guidelines, a company's "core activities" are those activities that "can be considered as the key operations necessary to achieve" the controller's goals. Article 29 Working Party Guidelines on Data Protection Officers ('DPOs'), § 2.1.2 (Dec. 13, 2016) [hereinafter Guidelines on DPOs]. The guidelines provide examples of what core activity does *not* include, such as IT support and paying employees, indicating that these activities are carried out by all organizations and

> …the GDPR imposes a new requirement on both controllers and those vendors with whom they contract to process personal data: the appointment of a data protection officer ("DPO").

while necessary or essential, are usually considered ancillary functions. *Id.* Unfortunately, the guidelines do not set forth a clear definition of "large scale," stating that a "standard practice" for what may be considered large scale may develop over time and until then, companies should consider a number of factors in making this determination. *Id.* § 2.1.3.[4]

A DPO must have "expert knowledge of data protection laws and practices," which will be considered in the context of the employer's particular processing operation and the protection required for such processing. GDPR art. 37(5). In other words, the more sensitive, complex and substantial an employer's data processing is, the more qualified its DPO must be. The functions of the DPO may be performed by an employee of the employer or data processor, or by a third party service provider. *Id.* at art. 37(6). Where a company has multiple subsidiaries, it may appoint one (1) DPO so long as he or she is "easily accessible from each establishment." *Id.* at art. 37(2).

It is critical that an employer carefully consider who to appoint as its DPO, as this individual holds a variety of significant responsibilities and rights. Specifically, a DPO is responsible for at least the following:

- Informing and advising the employer (or its data processor) and its employees of their obligations to comply with the GDPR and other data protection laws;
- Monitoring compliance with the GDPR and other data protection laws, including assigning internal responsibilities, training data processing staff, and conducting audits;
- Advising with regard to data protection impact assessments when required under Article 35;
- Cooperating with the employer's designated supervisory authority and serving as the contact point for the supervisory authority on issues relating to the processing of personal data;
- Serving as a contact person for employees with regard to "all issues related to processing of their personal data and to the exercise of their rights" under the GDPR; and
- Being available to consult, where appropriate, on any other matter.

[4] The guidelines do provide several examples of large scale sensitive data processing, including a hospital's processing of patient data, as well as some examples of non-large scale processing, such as an individual lawyer's processing of criminal convictions. *Id.*

Id. at art. 39(1)(a)-(e), 38(4). Moreover, a DPO is afforded the following rights:

- Insistence upon company resources to fulfill his or her job functions and to maintain ongoing training;
- Access to the company's data processing personnel and operations;
- Significant independence in the performance of his or her job functions;
- A direct reporting line to the company's highest management level;
- Ability to perform other tasks and duties provided they do not create conflicts of interest; and
- Job protection (i.e., the DPO "shall not be dismissed or penalized by the controller or the processor for performing his [or her] tasks").

Id. at art. 38(1)-(3), (5)-(6). The Article 29 Working Party guidelines reaffirms that a company may not terminate or otherwise penalize its DPO for providing advice with which the company does not agree if it is within the scope of his or her responsibilities. Guidelines on DPOs, § 3.4. Given the wide range of responsibility and authority afforded to a DPO, employers should look to this guidance as they appoint and train their DPOs.

f. New Notification Obligations for Personal Data Breach

An employer may take all appropriate steps under the GDPR to process its data and nevertheless find itself victim to a data breach. In this event, the GDPR provides more clarity than did the Directive, as it explicitly defines "personal data breach" and sets forth the employer's notification requirements. A personal data breach is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed." GDPR art. (4)(12). This definition is different from, and more expansive than, most U.S. state breach laws, which are typically only triggered upon exposure of information that can lead to fraud or identity theft.

In the event of a personal data breach, employers must notify the supervisory authority "competent" under Article 55 "without undue delay and, where feasible, not later than 72 hours after having become aware of it." *Id.* at art. 33(1). If an employer fails to provide the requisite notice within 72 hours of the breach, it must provide reasons for the delay. *Id*. Looking to Article 56(1), the competent supervisory authority may be the authority of the Member State where the employer has its main or only establishment. *Id.* at art. 55(1), 56(1); see also Guidelines on DPOs, § 2. Therefore, businesses that operate in the EU and/or process data across multiple jurisdictions will have to designate their "main establishment" to ensure that the proper authorities are notified, or else risk facing steep penalties, as discussed below. Further, companies will want to create internal policies (if they have not done so already) that defines what it means to become "aware" of a breach.

Notification must include, at a minimum, the following: (1) a description of the nature of the personal data breach, including the number and categories of employees and personal data records affected; (2) the DPO's contact information; (3) a description of the likely consequences of the personal data breach; and (4) a description of how the employer proposes to address the breach, including any mitigation efforts. GDPR art. 33(3)(a)-(d). If an employer does not have all of this information at once, it may provide the information in phases. *Id.* at art. 33(4). The GDPR requires that employers document any personal data breaches "comprising the facts relating to [the breach], its

effects [,] and the remedial action taken" so as to demonstrate compliance with the notification requirements. *Id.* at art. 33(5).

An employer need not notify the supervisory authority of a personal data breach where the breach is "unlikely to result in a risk to the rights and freedoms of [its employees]." *Id.* at art. 33(1). Of course, how this will be interpreted remains to be seen. On the other hand, where a breach is "likely to result in a high risk to the rights and freedoms" of the individuals whose data is being processed (*e.g.*, employees), an employer must also communicate information regarding the breach to the affected employees "without undue delay." *Id.* at art. 34(1). This communication must describe "in clear and plain language the nature of the [breach]" and contain, at a minimum, the name and contact information for the DPO; the likely consequences of the breach; and the measures taken or proposed to be taken to address the breach. *Id.* at art. 34(2). However, an employer need not communicate a breach to the employee (1) where the employer has "implemented appropriate technical and organisational protection measures" that rendered the data "unintelligible to any person who is not authorized to access it, such as encryption"; (2) where the employer takes subsequent actions to "ensure that the high risk to the rights and freedoms of [employees]" is unlikely to materialize; or (3) when notification to each affected employee would involve "disproportionate effort," in which case alternative communication measures may be used, such as public communication. *Id.* at art. 34(3)(a)-(c).

Data processors are obligated to notify data controllers (*i.e.*, employers) of a personal data breach "without undue delay after becoming aware of [the breach]," which would, of course, immediately trigger the employer's notification obligations. *Id.* at art. 33(2). It is important for employers to include in any agreement with its data processor a definition for "becoming aware" of the breach so that both entities may ensure compliance with this provision. *Id.*

g. Cross-Border Data Transfers

Similar to the Directive, the GDPR allows for data transfers to countries outside of the EU whose legal regime is deemed to provide an "adequate" level of personal data protection, as determined by the European Commission. *Id.* at art. 45. In other words, the third country or specified employer must ensure a level of protection "essentially equivalent to that ensured within the [EU]." *Id.* recital (104). In the absence of an adequacy decision, however, transfers may still be permitted where the employer implements certain appropriate safeguards, including:

- Legally binding and enforceable instruments between public authorities or bodies;
- Binding corporate rules ("BCR") in accordance with article 47;
- Standard contractual clauses adopted by the Commission, or adopted by a supervisory authority and approved by the Commission;
- An approved code of conduct pursuant to article 40; or
- An approved certification mechanism pursuant to article 42.

Id. at art. 46(2)(a)-(e).

With respect to BCRs, a company must first obtain approval from the appropriate supervisory authority (likely the authority of the Member State where the employer has its main or only establishment). *Id.* at art. 47(1). At a minimum, the following must be included in all BCRs: structure and contact details for the concerned group; information regarding data and transfer processes; how the rules apply general data protection principles; complaint procedures; and compliance mechanisms. *Id.* at art. 47(2). Unlike the Directive, the GDPR explicitly

provides that BCRs are a valid method of ensuring appropriate safeguards for cross-border data transfers.

With respect to codes of conduct, drafts of such code(s) must be submitted to the appropriate supervisory authority for approval and should, at least, address the following: (a) fair and transparent processing; (b) the legitimate interests pursued by employers in specific contexts; (c) the collection of personal data; (d) the pseudonymisation of personal data; (e) the information provided to the public and to employees; (f) the exercise of the rights of employees; (g) information provided to and the protection of children; (h) general data protection obligations of employers, including privacy by design and measures to ensure security of processing; (i) notification obligations with respect to personal data breaches; (j) transfer of personal data to third countries; and (k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between employers and employees. *Id.* at art. 40(a)-(k). Companies should determine whether there is an existing approved code of conduct (or other certification scheme) that covers their processing activity and if so, adhere to it. The EDPB will make publicly available all approved codes of conduct. *See id.* at art. 40(11). This would reduce the time and expense of seeking approval from the appropriate supervisory authority. When a company adheres to an approved code of conduct, however, it subjects itself to compliance monitoring by a body accredited by the supervisory authority for having "an appropriate level of expertise in relation to the subject matter of the code." *Id.* at art. 40(1). While a company may question the need to subject itself to this authority, adherence to an approved code of conduct is a mitigating factor when the supervisory authority considers enforcement action via implementation of an administrative fine.[5] *Id.* at art. 83(2)(j). Where a company decides not to (or cannot) adhere to a pre-existing code of conduct, it would be prudent for it to compare existing codes of conduct against its own policies and make necessary changes to ensure its procedures are at least consistent with already recognized and approved codes of conduct, which may streamline its own approval process.

h. The Privacy Shield

The above discussion assumes that the country to which an employer wishes to transfer data has not been deemed adequate by the European Commission. Focusing on the United States, from July 2000 until October 2015, the U.S.-EU Safe Harbor Framework operated as a voluntary self-certification program that had been deemed adequate for overseas data transfer by U.S. companies who self-certified by implementing policies and procedures that mirrored European-level privacy protection.[6] Given concerns about the level of access government agencies had to such data, particularly in light of revelations about NSA spying, the Court of Justice of the European Union (CJEU) ultimately found that the Safe Harbor program did not adequately protect personal data and consequently invalidated the program. Case C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, 2015 EUR-Lex 62014CJ0362 (Oct. 6, 2015), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362.

---

5 As discussed in subsection (i) below, an employer may be liable for the actions of its processors and sub-processors and should therefore consider whether the vendors with whom it deals have codes of conduct or other certification mechanisms in place.

6 *See* Commission Decision 2000/520/EC of 26 July 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council of the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the U.S. Department of Commerce, 2000 O.J. (L 215) 7-47.

In June 2016, the European Commission officially adopted a new framework known as the Privacy Shield.[7] Similar to the Safe Harbor program,[8] the Privacy Shield allows organizations in the U.S. to self-certify their compliance and implement a number of specified principles in order to transfer and process data from the EU.[9] One of the biggest changes stemming from the Privacy Shield is the breadth of its enforcement powers as opposed to the U.S.-EU Safe Harbor. Sanctions may include, among other things, publication of findings, removal from the Privacy Shield, and the return or deletion of any personal information that was received under the Privacy Shield. *Id.* Annex, Supplemental Principles § III(11)(e)-(g). How the Privacy Shield's principles will play out remains to be seen, and companies should look for further guidance as it is made public. Companies should note too, though, that the Privacy Shield likely will face legal challenges that undermine its ability to serve as a convenient and predictive way to transfer data from the EU to the U.S., particularly based on continued concerns of U.S. government surveillance and the greater levels of protection required by the GDPR. *See*, *e.g.*, Statement of the Article 29 Working Party on the Opinion of the EU-U.S. Privacy Shield (Apr. 13, 2016). Employers should therefore be cautious about relying on the Privacy Shield and consider using other alternative safeguards in the meantime, such as BCRs, standard contractual clauses, or approved codes of conduct.

…the Privacy Shield likely will face legal challenges that undermine its ability to serve as a convenient and predictive way to transfer data from the EU to the U.S., particularly based on continued concerns of U.S. government surveillance and the greater levels of protection required by the GDPR.

i. The Right to be Forgotten and the Right to Data Portability

What should a company do when faced with an employee who requests that his or her data be erased? How does a company respond to an employee who switches jobs and asks that it transfer his or her data to the subsequent employer? These are two questions organizations may very well face once the GDPR starts to apply, as it creates two important new rights for employees: the right of erasure (a.k.a. the right to be forgotten) and the right of data portability. At the same time, these new rights are potentially more onerous for employers, as they will be required to develop

---

7 *See* Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95-46-EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176) O.J. (L 207) 1-112. [hereinafter Privacy Shield].

8 Just as the former Safe Harbor program was not included in the language of the Directive, the Privacy Shield is not part of the GDPR.

9 It includes the following principles, similar to those of the GDPR, to which a company must adhere in order to self-certify: (1) notice; (2) choice; (3) accountability for "onward transfer" (*i.e.*, when transferring data to a third party, enter into a written contract requiring that the third party provide the same level of protection as required by the Privacy Shield); (4) security; (5) data integrity and purpose limitation; (6) access; and (7) recourse, enforcement and liability. Privacy Shield, § 2.1. If, however, it is "necessary to avoid prejudicing the ability of the organization in making promotions, appointments, or other similar employment decisions," an organization need not offer notice and choice to the employees. Privacy Shield, Annex, Supplemental Principles, § II (9)(b)(iv). Of course, how this language will be interpreted remains to be seen.

the capabilities to provide employees with GDPR-compliant data transfers.

The right to be forgotten requires an employer to erase an employee's personal data without undue delay in certain situations, including upon the employee's request or withdrawal of consent, or where the personal data is "no longer necessary in relation to the purposes" for which it was initially obtained and/or processed. GDPR art. 17(1)(a)-(f). Where the employer has made the personal data public, the employer must take "reasonable steps," taking into account "available technology and the cost of implementation," "to inform [entities] which are processing the data that the employee has requested the erasure by such [entities] of any links to, or copy or replication of, those personal data." *Id.* at art. 17(2). The employer is also obligated to communicate any such erasure to each recipient to whom the personal data had been disclosed, "unless this proves impossible or involves disproportionate effort." *Id.* at art. 19. This right is tempered by certain exceptions, including where the processing is for "archiving purposes in the public interest" or scientific, historical research or statistical purposes. *Id.* at art. 17(3)(a)-(e).

The right to data portability affords a data subject the right to receive personal data concerning him or her in a "structured, commonly used and machine-readable format and have the right to transmit those data to another [employer] without hindrance from the [employer] to which the personal data have been provided. . . ." *Id.* at art. 20(1). The Article 29 Working Party's Guidelines on the right to data portability makes clear that this right applies only to data that was "provided by"[10] the data subject and processed by automated means. Article 29 Working Party Guidelines on the right to data portability, § III (Dec. 13, 2016) [hereinafter Guidelines on the right to data portability]. In exercising this right, a data subject also has the right to have his or her personal data "transmitted directly from one controller to another, where technically feasible." GDPR art. 20(2). Consequently, companies will have to coordinate with one another to standardize their respective data formats to adequately respond to data subjects' requests for transfer while at the same time protecting its systems from becoming more vulnerable to breaches. This format "should always be chosen to achieve the purpose of being interpretable" and to produce "interoperable systems, not [necessarily] compatible systems." Guidelines on the right to data portability, § V.

This, in turn, may raise concerns for companies who have to work with competitors, particularly with respect to competition and the protection of intellectual property and other confidential information. Unfortunately, the Article 29 Working Party has not yet offered much guidance as to how companies may ease such concerns, simply stating that the employer "is responsible for taking all the security measures needed to ensure that personal data is securely transmitted (*e.g.*, by use of encryption) to the right destination (*e.g.*, by use of additional authentication information)." *Id.* Accordingly, employers that must respond to portability requests should "as a best practice, recommend appropriate format(s) and encryption measures to help the [employee]" maintain security. *Id*. In light of this, companies should take a risk-based approach to the data portability requirement and implement a variety of procedural safeguards.

Employers should be aware that the GDPR affords greater rights and protections to employees than did the Directive, as evidenced by its data quality principles, secure processing requirements, and employees' increased right of access. GDPR art. 15; *see also, e.g.,* recitals

[10] This may include data beyond that knowingly provided by a data subject. For example, a data subject may be considered to have provided data that was generated as a result of using a service or device, including search history, location data, and browsing behavior. *See* Guidelines on the right to data portability, § III.

(58)-(63). Accordingly, companies will have to implement internal processes to clearly and effectively facilitate the exercise of employees' rights under the Regulation and document all steps taken regarding such data so that a supervisory authority will be able to consider such actions when assessing GDPR compliance. If not, employer-employee relations

> …the GDPR affords greater rights and protections to employees than did the Directive, as evidenced by its data quality principles, secure processing requirements, and employees' increased right of access.

may suffer when an employer finds itself unable to comply with an employee's request to erase his or her personal data. This ultimately can hinder other processing operations, as other employees may be hesitant to share personal data knowing their rights may be violated at the end of the day. Companies can get ready for the GPDR now by assessing where it stores data, evaluating the type of data it has collected, and implementing a system that can generate these transfers. This may prove to be costly for many companies, particularly those operating on a small scale, as it will require significant effort and resources to develop these capabilities. At the same time, employers should weigh this cost against the risk of its employees refusing to provide or demanding the return of their personal data.

j. Liability and Penalties

In general, as controllers of personal data, employers are liable for damage caused by processing which "infringes" on the GDPR. *Id.* at art. 82(2). Processors, on the other hand, are only liable "where it has not complied with the obligations of the GDPR specifically directed to processors or acted outside or contrary to lawful instructions of the controller." *Id*. If there are joint judicial proceedings, liability may be apportioned according to the employer's and processor's respective responsibility and one entity may seek indemnification from others where appropriate. *Id.* at recital (146). Employers must be aware of how their relationship with processors, and those third parties with whom its processors contract, may impact the parties' respective liability.

Article 28 of the GDPR governs the relationship between controllers, processors, and sub-processors. Specifically, Article 28(1) provides that "where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject." Article 28(2) provides that "the processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes."

But what does this all mean? In essence, employers must conduct due diligence on their vendors to ensure that those processors also have the necessary policies and procedures in place to lawfully process data under the GDPR. While data processors already are subject to many requirements imposed by the GDPR, Article 28 puts the onus on the employer to ensure that its processor is meeting those obligations. Accordingly, employers should start to analyze and, where necessary, amend its existing relationships with vendors that are

processors to reflect the GDPR's principles and thus avoid being held liable for a processor's lack of compliance. For example, an employer may want to carry out a data protection impact assessment to assess the risks involved in processing and implement appropriate safeguards. *Id.* at art. 35. Regarding liability for

> …employers must conduct due diligence on their vendors to ensure that those processors also have the necessary policies and procedures in place to lawfully process data under the GDPR.

sub-processors, the language of Article 28 is not immediately clear as to how far down the processor chain an employer's or its processor's responsibility extends. Employers should look for further guidance to see how these provisions will be interpreted and in the meantime, be aware of how any sub-processors with which they work intends to comply with the GDPR.

Unlike the Directive, the GDPR imposes hefty penalties on an employer found to have unlawfully processed data. Based on the seriousness of the violation, there are two (2) tiers of penalties:

- Tier One: imposes a fine equivalent to 4% of a company's worldwide annual turnover or 20 million euros, whichever is higher;
- Tier Two: imposes a fine equivalent to 2% of the company's worldwide annual turnover or 10 million euros, whichever is higher.

Id. at art. 83 (4), (5).

Articles (83)(4) and (5) provide examples of violations that would subject an employer to each tier. For instance, an employer that violates an employee's rights (*e.g.*, failure to adequately respond to a request to erase an employee's personal data), fails to obtain employee consent for processing, or fails to otherwise lawfully process data will be subject to a higher level fine. Examples of violations that would subject a company to a lower level fine include the failure to properly notify the supervisory authority and/or employee of a personal data breach, or failure to designate a DPO. The GDPR sets forth certain mitigating factors, indicating that intent (or lack thereof) will play a role in determining the appropriate fine. *Id.* at art. 83(2). To better understand how this would play out, consider the following hypotheticals:

Hypo #1: Company is an "app" developer who collects its employees' personal data. It recently opened an office in the EU, which wants to share its employees' data with the Company's U.S. headquarters. The EU office transfers its employee data to the U.S. office without adhering to a standard contractual clause or other safeguard, and does not notify its employees' prior to transferring such data. Further, it does not document the reasons for its decisions not to adhere to standard contractual clauses or adopt other measures. The Company may be subject to a higher level fine for violating its employees' rights and failing to properly engage in cross-border data transfers.

Hypo #2: Same situation as above, except that Company is well-aware of its obligations under the GDPR. It carefully tracks and records its data processing operations and its DPO oversees every step. The Company's EU office adhered to an approved code of conduct when transferring its employees' data to the U.S. office and properly obtained consent to process the data for contractual purposes. In addition, the Company also documented how such purposes for processing fit within the derogations.

However, the Company suffered a data breach. It focused on containing the breach and securing its system, and therefore was not able to notify the supervisory authority of the breach until the following week. The Company may be subject to the lower level fine, as it failed to notify the supervisory authority of the personal data breach within 72 hours but had the proper mechanisms in place. Certain mitigating factors may reduce the fine, including the existence of such mechanisms, the unintentional nature of the violation, and an explanation for the delay.

The GDPR provides that these are the maximum fines that may be imposed, and that fines are not compounded for multiple violations arising from the same incident. *Id.* at art. 83(3). If the GDPR does not impose an administrative fine for infringements, or for other special cases, Member States may implement their own penalty systems, which may involve criminal penalties under the laws of that state. *Id.* at art. 83(7), (9). Moreover, employees may seek monetary damages from their employers. *Id.* at art. 82. Given the broad scope of liability an employer potentially faces, and the accompanying fines, it is exceedingly important for companies to take proactive steps now to ensure compliance with the GDPR come May 25, 2018.

D. What's Next?

So, what should you do now to prepare for the GDPR? Here are some suggestions:

- Conduct an internal audit and gap assessment
- Appoint a DPO
- Closely review existing processing procedures and modify where necessary
- Closely review existing vendor agreements and modify where necessary
- Determine permissible purposes for processing employee data
- Review employee notices and employment contract templates and modify where necessary
- Review (and/or implement) data breach notification policies and procedures
- Follow for updated GDPR guidance

Overall, it is crucial for your company to closely review its particular data processing operations to determine the level of training and sophistication required for your DPO and processing procedures. Companies should develop privacy regimes with an eye toward the technology they use and how it works for them, ensuring that "data privacy by design" is the touchstone of its operations. Be sure to properly and adequately vet any processing agreements between you and the companies with which you contract (and subcontract) to reduce the risk of vicarious liability. It is important for companies to update its notices of processing and understand what purposes are permissible given the difficulty in demonstrating valid consent. Most importantly, companies should continue to look for guidance from the Article 29 Working Party and specific Member States' DPAs as they offer insight into how the GDPR will be interpreted going forward, particularly given Member States' ability to ascribe higher protections to employment data. Employers are strongly urged to consider taking a multi-faceted approach to compliance given the uncertainty surrounding the consent specifically, and how the Regulation will be interpreted in general. There is a lot to do before May 25, 2018 – the time to prepare is now.

Proskauer.com

Beijing | Boca Raton | Boston | Chicago | Hong Kong | London | Los Angeles
New Orleans | New York | Newark | Paris | São Paulo | Washington, D.C.