Addressing Human Resources Data Flows In light of European Data Protection Board Recommendations

Nancy Lowrance
Lynn Goldstein
Martin Abrams

March 2021

Introduction

The leading global data protection issue for the past three decades has been personal data transfer governance. The most basic business processes require data to flow, and regulators, legislators and courts have struggled to figure out how data might be protected over distance and time. Originally, the issues were limited to the potential for private sector misuse of personal data and the lack of data security outside the jurisdiction where the personal data was collected. Now, the issues also include the ability of foreign national security agencies to obtain personal data held by the private sector. The jurisdiction that has expressed the most concern is the European Union (EU). The EU General Data Protection Regulation (GDPR) allows the transfer of personal data to a third country that ensures an adequate level of protection.[1] Since only a handful of countries have been found to have an adequate level of protection, there are other mechanisms in the GDPR to transfer personal data to a third country.[2]

Schrems II

The Court of Justice of the European Union (CJEU) in Schrems II held that in the absence of a decision determining that a third country ensures an adequate level of protection under Article 45(3) of the GDPR, personal data may be transferred to a third country only if "adequate safeguards" have been provided and that if transfers are being made pursuant to Article 46 of

[1] GDPR Article 45(1)
[2] Id. Articles 46 – 49 (e.g., transfers subject to appropriate safeguards, binding corporate rules, derogations)

the GDPR (e.g., Standard Contractual Clauses (SCCs)), then appropriate safeguards must be capable of ensuring a level of protection essentially equivalent to that which is guaranteed within the EU. Because the CJEU did not say what those appropriate safeguards are, the European Data Protection Board (EDPB) published on November 11, 2020 two documents for comments: Recommendations on supplemental measures for data transfers pursuant to the ruling of the CJEU in Schrems II and Recommendations on European Essential Guarantees for Surveillance Measures (collectively the Recommendations).

The Recommendations set forth a roadmap of steps to take in order to find out whether supplemental measures need to be put in place and a non-exhaustive list of supplemental measures. In setting forth the roadmap, the Recommendations provide elements which have to be assessed to determine whether the legal framework governing access to personal data in a third country can be regarded a justifiable interference or not. This assessment must be based on legislation that is publicly available and should not be based on subjective factors such as the likelihood of public authorities' access to data in a manner not in line with EU standards. The Recommendations suggest that such risk assessments should be based on the possibility of a request not the probability that such a request would ever take place. While supplemental measures such as encryption and other forms of technical obscurity may protect data in transit and at rest, if records need to be seen in a form that is identifiable in a third county that has not been found to provide a level of protection essentially equivalent to that guaranteed within the EU, then under the Recommendations supplemental measures must be in place that provide that level of protection. Under Schrems II and the Recommendations, it may be impossible to both provide that level of protection and make identifiable records available.

If global companies that operate in the EU put in place supplemental measures required by the Recommendations, operational impediments would be created related to the most basic business process, human resources (HR). The overarching conclusions of the CJEU in Schrems II are that the inappropriate collection of personal data by foreign (i.e., third country) intelligence services amount to an interference with the fundamental right to private life[3] and that European citizens have the right to redress if such interference takes place. Supplemental measures are intended to limit exposure if the laws where the data has been transferred are not deemed adequate.

Recital 4 of the GDPR provides that the right to the protection of personal data must be balanced against other fundamental rights, including the individual's freedom to choose an occupation and

[3] Charter of Fundamental Rights of the European Union, Article 7

right to engage in work[4] and the organization's freedom to conduct a business.[5] The IAF has argued that this balancing also must include the risk that data that pertaining the individual in a specific application would be accessed by a government entity inappropriately. To understand that such a balancing process was undertaken with competency and integrity, it is useful to understand a business process, the type of data used for a business process, and the risk that such data would be attractive to a government agency outside the EU.

The Recommendations

The EDPB states that Use Cases 6 and 7 are scenarios in which "*no effective measures could be found*."

- Use case 6: Transfer to cloud services providers or other processors which require access to data in the clear.

88. A data exporter uses a cloud service provider or other processor to have personal data processed according to its instructions in a third country.

If

1. A controller transfers data to a cloud service provider or other processor,
2. The cloud service provider or other processor needs access to the data in the clear in order to execute the task assigned, and
3. The power granted to public authorities of the recipient country to access the transferred data goes beyond what is necessary and proportionate in a democratic society,

Then the EDPB is, considering the current state of the art, inescapable of envisioning an effective technical measure to prevent the access from infringing on data subject rights. The EDPB does not rule out that further technological development may offer measures that achieve the intended business purposes, without requiring access in the clear.

89. In the given scenarios, where unencrypted personal data is technically necessary for the provision of the service by the processor, transport encryption and data-at-rest encryption even taken together, do not constitute a supplementary measure that ensures an essentially equivalent level of protection if the data importer is in possession of the cryptographic keys.

[4] Id. Article 15
[5] Id. Article 16

- Use case 7: Remote access to data for business purposes.

90. A data exporter makes personal data available to entities in a third country to be used for shared business purposes. A typical constellation may consist of a controller or processor established on the territory of a Member State transferring personal data to a controller or processor in a third country belonging to the same group of undertakings, or group of enterprises engaged in a joint economic activity. The data importer may, for example, use the data it received to provide personnel services for the data exporter for which it needs **human resources data**, or to communicate with customers of the data exporter who live in the European Union by phone or email.

If

1. a data exporter transfers personal data to a data importer in a third country by making it available in a commonly used information system in a way that allows the importer direct access of data of its own choice, or by transferring it directly, individually or in bulk, through use of a communication service,
2. the importer uses the data in the clear for its own purposes,
3. the power granted to public authorities of the recipient country to access the transferred data goes beyond what is necessary and proportionate in a democratic society,

Then the EDPB is incapable of envisioning an effective technical measure to prevent that access from infringing on data subject rights.

91. In the given scenarios, where unencrypted personal data is technically necessary for the provision of the service by the processor, transport encryption and data-at-rest encryption even taken together, do not constitute a supplementary measure that ensures an essentially equivalent level of protection if the data importer is in possession of the cryptographic keys.

Both Use Cases 6 and 7 are employed in the Human Resource Data (HR Data) context. What makes Use Cases 6 and 7 problems are the conclusions of the EDPB that "the power granted to public authorities of the recipient country to access the transferred data goes beyond what is necessary and proportionate in a democratic society." However, these conclusions should not apply to HR Data transferred from the EU to the U.S. The White Paper issued in September 2020 by the U.S. Department of Commerce, Department of State and Office of the Director of

National Intelligence states: "Companies whose EU operations involve ordinary commercial products or services and whose EU-U.S. transfers of personal data involve ordinary commercial information like employee records have no basis to believe U.S. intelligence agencies would seek to collect that data."[6] For example, U.S. government surveillance does not apply where the data transfer is of U.S. person data that is being communicated by one U.S. person (the data exporting American company) to another U.S. person (the data-importing company) located in the U.S.[7]

HR Data

Generally

Human resource management is data dependent, and those processes can be enormously complex. The governance of HR Data consisting of personal data has always been complex, in part because of the imbalance between the employer and the employee.[8] Therefore, HR Data cannot be governed by consent, and transfers may not be permissioned by consent either. Although, the Recommendations are broad in scope, this paper focuses on the transfer of HR Data and outlines specific examples that demonstrate how the Recommendations disrupt business models. Several global companies participated in the development of this paper. While the companies in this study are headquartered in the U.S., they have thousands of employees in the EU and operate in hundreds of countries. Collectively, these companies span the globe in industries such as pharmaceutics, hardware, software, and finance. Extensive business functions are performed in the EU which include, but are not limited to, HR, finance, contact centers, manufacturing, sales, and research and development.

Specific language in Use Cases 6 and 7 in the Recommendations is most troubling when applied to day-to-day HR business operations. As mentioned above, the EDPB states, in Use Cases 6 and 7, that "no effective measures can be found for these two scenarios." Real world examples that involve data flows and access to data for human HR Data demonstrate how the Recommendations limit the opportunities available to employees in globally integrated companies and constrain such companies from performing functions that are required to manage their operations, support their employee base and acquire future talent.

---

[6] Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after *Schrems II, at 2* [hereinafter White Paper].

[7] Alan Charles Raul, *Why Schrems II Might Not be a Problem for EU-U.S. Data Transfers,* Lawfare, December 21. 2020, https://www.lawfareblog.com/why-schrems-ii-might-not-be-problem-eu-us-data-transfers [hereinafter Raul]

[8] GDPR Recital 43

HR Data of global companies generally are managed in four ways:

1. Employees in the EU are supervised by people in the EU, e.g., the employee's direct supervisor and possibly one level above.
2. Employees in the EU are supervised by people in the U.S.
3. Employees in the EU are supervised by people in a country other than EU or U.S.
4. Employees in a country other than the EU or U.S., e.g., employees in Singapore, are supervised by people in the EU.

No matter where the employee works, this study found that employees ultimately report to executives and higher management in the country where the company is headquartered (for this study the U.S.) This web of reporting chains is how globally integrated companies are organized to leverage talent, optimize cultural environment and achieve customer expectations.

The employee life cycle management is a robust, structured framework that contains various processes from joining a company to leaving a company. Outlined below are real business scenarios that demonstrate the need for clarification and revision of the Recommendations in order for companies to manage their business and support their employees with training, compensation and benefits.

<u>Joining a Company</u>

- Recruitment
    - Recruitment is generally centralized in the U.S. with some local independence based on job function. In order to recruit potential employees, companies want to find and hire the most qualified candidate for the available position. In response, the individual data of an EU candidate flows to the U.S. company either directly or through a recruiter for submission and evaluation.
- Hiring
    - Background Checks (BC) generally are performed by third-party global vendors. The third-party vendors provide a go/no go assessment by individual candidate's name, but with proper authority, additional details can be obtained and accessed by U.S. employees. Care is taken so that appropriate data collection and sharing occurs and so that local laws are followed. For example:
        - A Brussels candidate submits their resume to the U.S. company who then sends the candidate's information to the third-party

vendor for BC. The third-party vendor stores the information in the U.S.

- For an EU employee who applies for a U.S. job that requires a BC, the global third-party vendor uses a local company to run a BC using the U.S. standard. The results are provided back to the U.S.

- Conversations (written, verbal, video) are conducted with individuals across the globe in the hiring process to discuss the pool of candidates and to determine the most qualified candidate.

- Onboarding
  - Onboarding is the process of integrating the new employee into the company and making the employee familiar with the company's culture. This process often involves access to systems, training, benefits, expectations, and office location. As a part of the process, the employee shares personal information in written correspondence, email, and direct entry into company systems. This information then is shared, with appropriate access controls, within the company, as well as with third-party vendors, for the purposes of providing access to systems, payroll and enrolling in benefits.
  - Single sign on is utilized so employees can obtain needed access to systems and tools. All of the employee's credentials are loaded into a global system for access and authentication. Access to these systems is essential for payroll, benefits, time reporting and training.

<u>Performance Management and Compensation</u>

The cyclical performance management process involves three key assessments:

- An individual's performance assessment
- Relative assessment against peers
- Relative assessment at the same level across the organization

This is a global process where performance and compensation information require the flow of an individual's information so that it can be shared and discussed with management and HR across the globe through a variety of communication methods including phone, email and video chat. These detailed conversations evaluate an individual's performance and how an individual has performed as compared to others within the organization. In addition to current performance, the potential of the employee is discussed in order to determine career path, training needs and job growth opportunities. This process evaluates and rates employees comparably across the

world and sets the stage for compensation analysis and pay treatment that is harmonized to treat people fairly and equally.

Talent and Succession Planning

These companies consider people as their most important asset. Employers help employees feel engaged and motivated to perform their individual work. The goal of the talent process is to identify employees with a certain amount of readiness for key leadership roles and specific development plans to achieve that end result. The objective is to acquire the best talent in the right seat. If sharing across country borders for a centralized view of the talent bench is not allowed on an individual basis, then there are real impacts to the business which places major business objectives at risk, and the world of opportunity for EU employees becomes much smaller.

Training

Training is often delivered globally across the organization, and in some cases, it is required and regulated. Reporting of details, related to which courses are required by job function, who took the training, when they took it, and when they completed it, are required. If unable to perform this function, there would be a significant regulatory impact for some companies.

Benefits and Health

Global HR systems contain information that needs to be updated by the employee. Information, such as beneficiaries, contacts in case of incidences, marital status and home address, need to be provided. These global systems need to be accessed from anywhere, and the data generally are stored in the U.S.

Other Examples

Emergency Situations

Companies prepare for potential emergency situations such as tornadoes, hurricanes, and tsunamis. As part of that process, supervisors must have the contact information for each of their employees so they can be reached to confirm their safety. If the employee cannot be reached, other measures are implemented.

Active Directory

Large companies generally maintain an intercompany directory that can be accessed by any employee from anywhere in the world. This directory contains information, such as contact information, reporting structure, and location, for every employee worldwide. This information

is a vital resource to employees for many reasons, including contacting an individual, escalating an issue or identifying someone in an organization that can be of assistance.

Volunteer Programs

Employees volunteer for programs that allow them to utilize their skills for humanitarian efforts in, for example, marketing, technology, construction, and legal. Employees apply for these opportunities and their applications are reviewed in the U.S. If selected, EU employees visit the U.S. to engage with their cohorts prior to departing for their destinations. Programs like this could not work if organizations were unable to transfer information about EU based employees to the U.S. for reporting and updates. Corporate social responsibility and giving back to the community are intrinsic commitments made by many organizations.

Customer Support

Service Level Agreements (SLAs) define the level of service expected from a third-party vendor. The language outlines specific metrics including what service is being measured, duration of time for resolution and associated remedies or penalties. In order to meet these expectations, companies provide 24x7 support all over the globe, and their employees share their contact information with customers as a normal course of business.

Centralization, Storage and Access of HR Data

With a centralized architecture, there is more efficiency for performing data analysis, corporate management oversight and providing effective security controls. Data are primarily stored in one or more of these ways: 1) In house, 2) Cloud providers and/or 3) Software as a Service provider and can be accessed globally. The third-party companies provide needed services and are integral stakeholders for operations of large global companies. If HR Data are not allowed to be shared, massive problems will be created, as outlined above, for companies with U.S. operations. Even if an employee is EU based, the HR Data still will be flowing to the U.S. with the U.S. holding the encryption keys.[9]

The Test Set Forth in the Recommendations is Unreasonable

The EDPB concludes in Use Cases 6 and 7 that the power granted to public authorities of the recipient country to access the transferred data goes beyond what is necessary and proportionate in a democratic society. In order to determine the legal framework governing access to personal data by public authorities in a third country, according to the Recommendations, the data exporter and data importer should look into objective factors and

[9] See comments on EDPB recommendations filed by Workday and Salesforce.

not rely on subjective ones such as the likelihood of public authorities' access to data.[10] In the U.S., data exporters and data importers of HR Data are relying upon an objective test because the U.S. Government has said that "Companies whose EU operations involve ordinary commercial products or services and whose EU-U.S. transfer of personal data involve ordinary commercial information like employee records have no basis to believe U.S. intelligence agencies would seek to collect that data."[11] But if this statement by the U.S. Government is not adequate, then companies also should be able to look into subjective factors such as the likelihood of public authorities' access to data. To prohibit companies from making such an inquiry would undermine the fundamental rights and freedoms of EU individuals.

Recital 4 of the GDPR provides that the "right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects **all** fundamental rights and observes the freedoms and principles recognized in the Charter as enshrined in the Treaties . . . ."[12] The Charter of Fundamental Rights recognizes the freedom to choose an occupation and the right to engage in work. As the discussion of HR Data above demonstrates, the freedom to choose an occupation and the right to engage in work are degraded when the right to protection of personal data is preferred even though there is little risk to them. If EU employees are precluded from being considered for positions in a third country because their HR Data cannot be shared in their employer's cloud-based HR system, even though that third country has said there is no basis for the employer to believe that country's intelligence agencies would seek to collect that data, then the EU employees' fundamental rights are being violated.

In a risk-based system, the test set forth in the Recommendations goes too far. When the benefits to EU employees are weighed against the risks to EU employees, the benefits clearly outweigh the risks. Otherwise, the clear result of the Recommendations is localization of EU HR Data to the disadvantage of EU employees working for global companies. EU candidates will have a harder time being recruited by companies headquartered in a third country because it is more likely that the recruiter will be located where the company is located. Even if the candidate comes to the recruiter's attention, they may have less chance to be hired because of their location in the EU and the difficulties in accessing their data from the third country (even if they are the superior candidate). Even if the candidate does get hired, they will not see the full picture

[10] Recommendations ¶¶ 39 - 42

[11] White Paper at 2. Raul (Such companies are not "electronic communications service providers" that transfer data that may be legally targeted for collection. They are not in the business of transmitting (or storing) communications for third parties but rather are transferring their own customer, employee or business data from their bases in the EU to their bases in the U.S.)

[12] Emphasis added

of the company when they are onboarded; they will only see an EU version of systems and will not have access to the global systems. EU employees will be disadvantaged in performance management and compensation because they will not be able to be compared one on one to their peers outside the EU and because they will not be considered for positions outside the EU even if they want to be. Training and other coaching opportunities will be siloed in the EU. EU employees will not be able to see the full intercompany directory so they will not be able to see the reporting structure of colleagues and superiors and to see the location of other employees.

The freedom to choose an occupation and the right to engage in work is violated when the HR Data of EU employees working in the EU for a company in a third country cannot be transferred to that third country where there is "no basis to believe" their data will be sought by that country's intelligence agencies.[13] Likewise, the freedom to conduct a business is infringed.[14] Employers may not be able to hire the best candidates, and even if they are able to do so, they will not be able to offer EU employees the best opportunities because they will not be able to compare them to their peers around the world on a one-on-one basis and because they will not be able to consider them for positions outside the EU.

Conclusion

Recital 4 of the GDPR says that the "processing of personal data should be designed to serve mankind." By articulating a hyper-conservative test for determining when "the power granted to public authorities of the recipient country to access the transferred data goes beyond what is necessary and proportionate in a democratic society," the EDPB has preferred the right to the protection of personal data and has disadvantaged the freedom to choose an occupation and the right to engage in work and the freedom to conduct a business. The Recommendations have ignored the directive of Recital 4 to consider the right to the protection of personal data in relation to its function in society and to balance it against other fundamental rights. Too heavy a weight has been put on the data protection side of the scale which is balancing several fundamental rights.

The example of HR Data shows that the Roadmap and Use Cases 6 and 7 set forth in the Recommendation are more complex than articulated. In order to determine whether the power granted to public authorities of the recipient country to access the transferred data goes beyond

[13] There is no empirical evidence that personal data transferred from the EU to the U.S. under SCCs has been the subject of actual surveillance by U.S. intelligence agencies, and U.S. "national legislation" precludes targeting transfers between U.S. companies. Raul

[14] U.S. surveillance law expressly define U.S. corporations to be U.S. persons, and U.S. surveillance law may not be applied when U.S. person data or data related to persons located in the U.S., such as an entity at the importing end of the SCC transfer in the U.S. Raul

what is necessary and proportionate in a democratic society, the data importer and the data exporter should not be limited to the legislation itself and reported precedents. The way the intelligence agency in the third country exercises its power and that agency's articulation of its power should be considered. Otherwise, the risks will outweigh the benefits to the detriment of the individual, and it is the interests of the individual that the Recommendations are trying to protect. Using a too hyper-conservative test ends up not protecting the rights and freedoms the Recommendations were designed to protect.