EDPB Members:

These comments are respectfully submitted to the EDPB in connection with its public consultation on the draft Guidelines 01/2022 on Data Subject Rights – Right of Access ("draft Guidelines").

My Role

By way of background, I have over twenty years of experience in data protection, first as a Global Data Protection Officer for a Fortune 100 company with offices across the European Union, and currently, as a law firm partner exclusively handling data protection matters. From both an in-house and external data protection attorney perspective, I have assisted businesses in establishing their EU and global data protection frameworks, including in relation to handling subject access requests. Since 2002 and continuing, I have also had the honor of being a member of the International Working Group on Data Protection in Technology (IWGDPT/Berlin Group). I support that group as a Data Scientist, providing feedback from a corporate/business perspective on a variety of existing and emerging data protection topics.

Over the years, I have assisted employers with a great many subject access requests submitted by data subjects who are residents of the European Union and United Kingdom (and more recently, requests submitted by California consumers under the California Consumer Privacy Act of 2018). In a percentage of those situations, the EU and UK data subjects ultimately filed complaints with the relevant supervisory authorities. As such, I have interacted many times with the supervisory authorities in relation to subject access complaints.

Through my work on those matters, I have witnessed considerable uncertainty by employers in relation to providing highly sensitive employment-related records sought in connection with responding to subject access requests. In particular, this includes records pertaining to employee terminations and other disciplinary matters, those relating to investigations of compliance alert line matters, and those pertaining to crimes and other material violations of laws and/or company policies. Those types of documents are routinely sought by employees/former employees, yet many EU employers and other businesses remain unsure what has to be provided and what can legitimately be excluded under the GDPR.

I respectfully submit these comments for the EDPB's consideration, based on that experience.

EDPB's Subject Access Request Guidelines

The EDPB's draft Subject Access Request Guidelines provide very valuable information and direction for organizations with respect to complying with data subject access requests under the GDPR. Among other things, the Guidelines also underscore the critical importance of that right along with the corresponding expectations for fulfilling it.

While I commend the EDPB for addressing the right of access in the employment context as part of its draft Guidelines, I also urge the EDPB to consider adding additional information to the final Guidelines on that topic. Specifically, and as briefly noted above, it would be very helpful for EU and other employers if the EDPB included additional clarification in its final Guidelines on its expectations for providing copies of highly sensitive employment records in connection with subject access requests.

In doing so, the EDPB will also be assisting data subjects as well as the supervisory authorities. For example, when an employer responds to a subject access request in an insufficient manner, the data subject must either accept the response or file an appeal or complaint, which naturally requires more time and energy on his/her part. Similarly, when a complaint is filed with the supervisory authority, the agency must devote a portion of its investigator staff, administrative resources, and budget to addressing it. Logically, if there are clearer rules as to the types of employment records that can and cannot be accessed via a subject access request, this should help reduce the disputes about the records provided, and, in principle, lower the percentage of escalation of those matters to the supervisory authorities.

Main Category of Subject Access Requests --Employees/Former Employees

As the EDPB is likely aware, the vast majority of subject access requests under the GDPR are submitted by employees and former employees. Unquestionably, some of those requests are premised upon genuine concerns by those data subjects in relation to the treatment of their personal data held by their employer. At the same time, a notable portion of them (and possibly even the majority of them), are submitted by employees and former employees for reasons that are unrelated to data protection.

By way of example, many of the subject access requests are submitted by employees/former employees with documented, significant workplace performance issues. This includes, for example, employees who are in line for (or already have been) subject to 'for cause' terminations; those who have submitted workplace-related grievances (relating to issues that have no bearing on data protection); and those who have been subject to compliance investigations for a wide array of issues (e.g., financial, legal, discriminatory, and other violations which also have nothing to do with data protection).

Motivation Cannot Be Considered—Yet The GDPR Also Cannot Be Distorted

It is clear from the GDPR as well as the EDPB's draft Guidelines that a data subject's right to information must be fulfilled irrespective of any motives the data subject may have, and even in the context of the employment relationship.[1]

Nevertheless, the right to information, including that held by an employer, is not absolute. The GDPR contains certain limitations on the right of access such that it is not used excessively or inappropriately, including, for example, to infringe the rights of other data subjects.[2]

In that regard, the EDPB's draft Guideline notes in Footnote 7 that the limitation on considering a data subject's motive in connection with responding to a subject access request, "*is subject to any applicable national procedure rules adopted in accordance with GDPR Article 23, which relates to boundaries that member states can adopt in relation to court proceedings and other legal claims by parties in connection with their legal relationship*." (Italics added.)[3]

In connection to this point, I call on the EDPS to recognize that in addition to the limitations imposed by Member State law, *the GDPR itself* must also be interpreted in a way that does not disproportionately affect the rights of third parties in the context of subject access requests, and in particular the rights of employers and former employers. In other words, it would be illogical to assume that the drafters of the GDPR intended it to be available as a tool to disregard the boundaries of member state civil procedure rules or the rights of the employer and other members of its workforce.

As such, it would be very helpful for the EDPB to confirm in its final Guidelines that the GDPR is not intended as a tool to impair civil law claims or the discovery rules associated with those actions. These aspects of subject access rights are of particular importance in the employment relationship and in connection with disputes under labour law.

Examples of Employer Challenges in Fulfilling the Right of Access

EU-based employers are struggling to manage the risks created by the growing number of subject access requests submitted by employees/former employees, and to understand the proper scope of such requests. Among other things, the challenges that those employers face include:

- The recognition that employees/former employees involved in disciplinary or performance issues are much more likely than other, more neutral categories of data subjects to escalate

[1] Specifically, the Guidelines state that "controllers should not assess "why" the data subject is requesting access, but only "what" the data subject is requesting….and whether they hold personal data relating to that individual…." Draft Guideline, Section 2, Paragraph 13.

[2] GDPR Article 15(4), and Recital 63.

[3] Draft Guideline, footnote 7.

subject access requests, such as by filing complaints or lawsuits, if they feel that any records are improperly withheld.

- The fear that a national supervisory authority will find the employer to be in violation of GDPR Article 15, such as where the employer, in good faith, withholds sensitive employment records under an exemption.

- The awareness that a GDPR violation based on the right of access can result in highly unfavorable consequences for the employer, including, for example, fines of up to 4% of the organization's worldwide annual turnover or €20 million (whichever is higher), significant reputational damage, and a long-term impact on the relationship between the company and the supervisory authority.

- The recognition that an adverse outcome of a complaint filed by an employee/former employee—and, indeed, *any* suggestion of non-compliance included in the response to the data subject from the supervisory authority--can have a significant "spillover" effect with respect to other similarly situated employees/former employees across the organization.

- The challenge of identifying and extracting *all* relevant employment records from a wide variety of on-site and off-site storage locations including cloud storage locations and potentially, personal devices of relevant company personnel, while responding within the 30-day time period.

- The uncertainty as to how the very high level exemptions to the right of access under the GDPR are applicable in the context of sensitive employment records, and

- The uncertainty as to whether withholding any employment-related records (and even the most sensitive types as discussed in these comments), is worthwhile in the long run in light of the risk of appeals, complaints to the supervisory authorities, and lawsuits by the employees/former employees.

Based on these challenges, and in the spirit of transparency, employers often decide to provide employees/former employees with 'all' records (at least in redacted form) with the hope that the data subject will be satisfied with the response and not pursue an appeal, complaint, or lawsuit. Employees/former employees are well aware of the pressure on employers to take this approach, and have thereby seemingly found a GDPR-based avenue for document requests that often far exceeds legitimate routes established for data-gathering under the local Member State civil procedure and discovery laws.

Types of Employment Records Typically Sought and the Surrounding Uncertainty

Generally speaking, the uncertainty of employers relating to subject access requests is limited to certain categories of records that are often requested. Those records include, for example, statements gathered from line managers and human resource personnel about the employee's/former employee's poor performance, misconduct, disciplinary matters, compliance issues, or basis for termination. Naturally, the managers and other employee providing those statements to the employer do so with the expectation that the information will be held in strict confidence and will only be accessible to the small group of trained professionals evaluating the matter.[4]

Employers are similarly uncertain as to their responsibility to redact sensitive performance and compliance information from the records provided to the data subject. While redaction of the names of others and surrounding legal/compliance decisions may be possible in *certain* situations, there is an inherent risk of re-identification by the employee/former employee submitting the subject access request when only a handful of company employees are typically involved in these types of decisions—and when the job categories of those few individuals such as the line manager and relevant human resource personnel—are, in most cases, well known to the data subject.

Recommendations for EDPB Clarification of the Legal Uncertainty

It would be very helpful for the EDPB to consider including additional clarification as to its expectations for providing sensitive employment documents t encompassed within a subject access request. The clarification might include a breakdown of the types of employment-related records that would generally be within the proper scope of a subject access request, versus those that are normally exempt.

For example, the EDPS could consider the following:

- At one end of the spectrum, the employer is expected to provide copies of employment records containing the employee's personal data (which do not include information about other individuals and/or proprietary company trade secret, copyright or other legal or compliance opinions). Under that category, and absent a very compelling exception applicable to a particular record, employers are required to provide employees with copies of their personnel file, occupational health medical records, pay slips; disability records; vacation and sick time records; training records; copies of their job application and offer letter; copies of any disciplinary letters provided to the employee; employee compensation

[4] Any broader disclosure of that information, including to the employee/former employee himself/herself, would very likely discourage managers and other personnel from providing truthful and complete information to the employer, and could thereby compromise the integrity of performance and compliance processes at many organizations. In addition, such disclosures would also likely contradict company policies and data protection notices that describe the safeguards and limitations on access which are in place for that data.

records, benefits and pension information, tax deductions, and similar information that relates to the treatment of their data by the employer.

- At the opposite end of the spectrum, the employer is permitted to object to and withhold certain highly sensitive types of employment records, provided that the employer provides the data subject with information about the existence of those records and the legitimate basis for the exemption. This category includes, for example, copies of witness statements pertaining to compliance investigations or grievances, assessments by the employer pertaining to those matters or to other disciplinary issues including termination, and similar information collected in connection with suspected or actual commission of crimes or other material violations by the employee/former employee. In those situations, the employer should also consider whether partial redaction of the record, such as to exclude legal conclusions, other proprietary information, and the identities of other individuals (without their express or reasonably inferred consent), would render the document producible to the employee/former employee in relation to the subject access request. In doing so, the employer must keep in mind that the document should not be produced in redacted form where there is a reasonable risk of re-identification of the identities of those individuals by the recipient.

- In terms of the middle ground, it would be helpful if the EDPS could clarify the rules for employers to evaluate which records are and are not within the scope of the subject access request. For example, business-related emails that simply include the data subject's name as a recipient or sender should generally be out of scope as they do not contain personal data about the data subject. On the other hand, emails that contain additional personal information about the data subject, such as approval of his/her vacation time, requests to the employer to add of family members as dependents, and enrollment in company-provided social events, would be within scope.

- The EDPS may also want to address private emails sent by the employee using the company system, to the extent that they still exist. Employers recognize that once they determine that an email is of a private nature, they are not supposed to read it. Yet, they are uncertain whether those emails should or should not be produced in connection with a broad subject access request by an employee/former employee.

- As partially referenced above, the EDPS may want to clarify that while redaction should always be considered for employment-related compliance, legal and similar records as well as those including the identities and/or information provided by other persons who have not consented to the disclosure, redaction may be unlikely to offer sufficient protection in situations where there is a reasonable risk of re-identification.

- Finally, it would be helpful to reiterate that the GDPR is not intended to be used as a tool by employees/former employees or others, for bypassing member state laws relating to civil procedure and discovery.

Conclusion

In conclusion, there is a great deal of uncertainty by EU employers (as well as other businesses) in relation to the proper scope of employment records that fall within a subject access request. This uncertainty not only impacts the employer, but also the data subject and the supervisory authorities by raising the likelihood of complaints to supervisory authorities and requiring them to devote staff and other resources to evaluating and resolving them. It is possible that a number of these complaints could be avoided on a go forward basis by increased clarity for employers as well as data subjects with respect to the permitted scope of employment records within those requests.

Given the significance of the right of access issue in the employment context, the EDPB may also want to consider a separate consultation on that topic. That would allow the EDPB to gather information first-hand from relevant stakeholders such as the national supervisory authorities, EU employers, and data protection and human resource professionals handling those matters on a routine basis.

Thank you.

Respectfully submitted

Joan Antokol
Partner, Park Legal LLC