General Data Protection Regulation in U.S. Litigation through Mid-Summer 2019

By: Michael H. Gladstone

Mike Gladstone is a Director in McCandlish Holton PC's Litigation Practice Group, where he counsels clients in civil litigation and arbitration involving commercial, tort, immigration and employment disputes. He has extensive trial experience in the state and federal courts in Virginia, Washington DC, Maryland and New York. He has spoken and written on the implications of the GDPR for U.S. businesses and litigation. Mr. Gladstone is a member of the IADC and its employment law and international practice committees and the American Immigration Lawyers Association.

IN JANUARY 2012, the European Commission set out plans for data protection reform across the European Union. One of the key components of the reforms was the introduction of the General Data Protection Regulation (GDPR).[1]

The GDPR is a comprehensive set of rules designed to give European Union citizens more control over their personal data. The GDPR applies, generally, to any organization operating within the European Union, as well as organizations outside of the European Union which offer goods or services to customers or businesses in the European Union among others. Almost every major corporation in the world is affected by this legislation. This legislation came into force across the European Union in May 2018.

There has been considerable uncertainty how GDPR will be addressed in litigation commenced in the United States. However, as a year has passed, motions relating to

[1] Regulation (EU) 2016/679. The GDPR is available in English at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679 (last visited October 2, 2019).

GDPR are beginning to be adjudicated, and trends are starting to occur. This article provides a detailed summary of courts' treatment of GDPR-related arguments and summarizes the potential impact of GDPR on United States litigation.

I. Impact of GDPR currently

As of July 19, 2019, eleven federal cases reference "GDPR" or the "General Data Protection Regulation". No state court cases appear. Of the cases returned, four are from the United States District Court for the Southern District of New York,[2] and two are from California,[3] one from the Central District of California and the Northern District of California. The remaining five cases originate from District Courts in Washington, Maryland, Alabama, Utah, and Florida.[4]

These eleven cases generally involve discovery disputes, often in intellectual property matters. In these scenarios, the responding party has raised GDPR as a bar or impediment to a full discovery response. In general, courts have proceeded under a normal Rule 26 analysis in evaluating the discovery requests and/or objections, while paying additional attention to the objections involving the GDPR or similar and/or related European laws. The extent of the discussion of the GDPR hinges, generally, on the significance of the discovery sought and accuracy of the assertion of the regulation as a bar or impediment to the discovery sought. This discussion is often accompanied by an analysis of the evidence supplied by the objecting party related to the precise requirements and burdens of the GDPR on the party, the risks those requirements create for the party if responses were made as demanded, and the costs of complying with the requirements.

Not surprisingly, where respondents provided little specificity concerning the regulation or supporting evidence of

---

[2] *In re* Hansainvest Hanseatische Investment-GmbH, 364 F. Supp.3d 243 (S.D.N.Y. 2018); Morgan Art Foundation Ltd. v. McKenzie, No. 18 Civ. 4438 (AT), 2019 U.S. Dist. LEXIS 109997, at *1 (S.D.N.Y. July 1, 2019).

[3] Uniloc 2017 LLC v. Microsoft Corp., No. 8:18-CV-020530-AG, 2019 U.S. Dist. LEXIS 20933, at *1 (C.D. Cal. Feb. 5, 2019); Finjan, Inc. v. Zscaler, Inc., No. 17-cv-06946-JST (KAW), 2019 U.S. Dist. LEXIS 24570, at *1 (N.D. Cal. Feb. 14, 2019).

[4] *See* Ironburg Inventions, Ltd. v. Valve Corp., No. C17-1182-TSZ, 2018 U.S. Dist. LEXIS 142919 at *1 (W.D. Wash. Aug. 22, 2018); Cox v. Smith & Nephew, Inc., No. 1:18-cv-00326-CCB, 2018 U.S. Dist. LEXIS 128592 at *1, *54 (D. Md. July 31, 2018); d'Amico Dry D.A.C. v. Nikka Fin., Inc., No. CA 18-0284-KD-MU, 2018 U.S. Dist. LEXIS 179858, at *1 (S.D. Ala. Oct. 19, 2018); Corel Software, LLC v. Microsoft Corp., No. 2:15-cv-00528-JNP-PMW, 2018 U.S. Dist. LEXIS 172875, at *1 (D. Utah October 5, 2018); United States Soccer Fed'n, Inc. v. Silva Intn'l Invs., No. 19-21119-MC-Cooke/Goodman, 2019 U.S. Dist. LEXIS 75350, at *1 (S.D. Fla. May 2, 2019).

burdensomeness, the arguments received less credence. Some responding parties concede GDPR is not a bar to responding, but stress the costs of a GDPR-compliant response. However, given the level of the courts' discussion of the GDPR in these eleven cases, it is sometimes difficult to determine from the opinions the detail with which the regulation was briefed and argued. A review of selected discovery briefings suggests that arguments as to burden have not been significantly developed, for example through itemization of GDPR connected costs. Based on the cases so far, mere citation of the GDPR or another foreign state's data protection regime provides no categorical basis for relief from United States discovery.

Parties seeking discovery resist the responsive party's arguments grounded in the GDPR as vigorously as arguments grounded in any other basis offered to block or limit discovery. In the apparent interest of fairness, however, some courts have already added protective terms to discovery orders to limit the dissemination of personal or proprietary data, even where the reasoning leading to the court's decision would not have suggested it would implement such measures. In one case, shortly after the GDPR came into effect, the United States District Court for the District of Maryland acknowledged the parties' efforts to address issues arising under the GDPR by supplementing the protective order to add language governing the processing and handling of data from foreign custodians covered by the GDPR.[5]

II. Analysis of the Case Law

Of the eleven federal cases, eight seem worth exploring in greater detail. This article discusses these cases in chronological order below.

Ironburg Inventions v. Valve Corp. Three months after the GDPR went into effect, the United States District Court for the Western District of Washington addressed the GDPR and the European Convention on Human Rights (ECHR) in the context of deposition marking. In *Ironburg Inventions, Ltd. v. Valve Corp.*[6] the dispute concerned deposition testimony marked as confidential during a deposition. The parties disagreed as to which designations ought to continue to be confidential and require filing under seal and moved for different parts of the deposition testimony to either be placed under seal or de-designated.[7]

Ironburg raised the GDPR and the ECHR in arguing that its witness, Simon Burgess, a United Kingdom

[5] *Cox*, 2018 U.S. Dist. LEXIS 128592 at *1, *54.
[6] 2018 U.S. Dist. LEXIS 142919 at *1.
[7] *Id.* at *4.

citizen, was entitled to heightened protection of his personal information.[8] Ironburg argued certain medical information concerning Burgess' ability to testify competently and provide accurate answers was revealed in the deposition, and if the information were disseminated it would cause the witness persistent embarrassment.[9] Ironburg argued the medical information demonstrated good cause to maintain Burgess' deposition transcript under seal.[10] Any less restrictive alternative, Ironburg argued, would leave Burgess vulnerable to public embarrassment, as no portion of his deposition transcript could be disclosed without disclosing the medical condition because such information was "necessary to explain the context of his testimony."[11]

After reviewing the testimony in camera, the court ruled that Ironburg's arguments, including those founded on the ECHR and the GDPR, did not satisfy the standard of proof applicable to a party seeking to seal evidence, or even to maintain its confidentiality.[12] The court stated:

> Mr. Burgess' status as a citizen of the UK, without more, does not meet the compelling reasons test, as Ironburg has not shown how the EU laws relating to privacy or data protection renders the disputed experts protectable. Moreover, Mr. Burgess has already disclosed most of the allegedly sensitive "commercial information" discussed in the transcript in an attempt to obtain a positive review of his product. As a result, Ironburg's concern that the narrow portions of his testimony at issue in this motion contains confidential commercial information rings hollow.[13]

Nevertheless, the court allowed excision of the portions of the transcript containing medical or sensitive financial information.[14]

The court also considered a motion by Ironburg to seal a hearing transcript from the Patent Trial and Appeal Board, which allegedly contained sensitive health information.[15] Finding the limited references to the health information were already publicly disclosed by Burgess via tweet, the court denied this request.[16] Here, mere reference

[8] *Id.* at *5.
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *Id.* at *8-9.
[13] *Id.* at *9.
[14] *Id.* at *10.
[15] *Id.*
[16] *Id.* at *11.

to EU citizenship and the GDPR were found insufficient to secure confidential material, seal a portion of the record, or defend a confidentiality designation.

d'Amico Dry D.A.C. v. Nikka Financial. Two months after *Ironburg Inventions*, the United States District Court for the Southern District of Alabama also addressed the GDPR in the context of a deposition. In *d'Amico Dry D.A.C. v. Nikka Financial,*[17] the issue arose *before* the deposition occurred in a creditor's action to enforce a judgment in admiralty against an alleged "alter ego" of the judgment debtor.[18]

The defendant corporation, noticed for a videotaped Rule 30(b)(6) deposition, objected to the deposition on numerous grounds, including the corporate designee's individual refusal to consent to a videotaped deposition.[19] The corporate designee, a citizen of the European Union, claimed videotaping the deposition without his consent would violate his rights under the GDPR, the ECHR, and the Human Rights Act.[20] Specifically, the corporate defendant argued:

> captured video footage counts as personal data if the subject can be identified. Here, [corporate designee] will be identified in the videotaped deposition and, thus, under the Acts, d'Amico is required to obtain [corporate designee's] consent and signed release before d'Amico records, uses or stores video of him, otherwise d'Amico will be in breach of the law. [Corporate designee] has serious privacy concerns about the videotaping of his deposition as he thinks the only purpose of the video is to annoy, embarrass, and oppress him and violate his privacy interests. Thus, he does not consent to his deposition being videotaped.[21]

The court reviewed the foreign citations supplied by the defendant concerning the necessity of permission from the deponent before videotaping could occur, and found them inapplicable to a duly noticed and court authorized video deposition for use in domestic litigation.[22] The court further observed that the citations it was supplied—the content of which is

[17] No. CA 18-0284-KD-MU, 2018 U.S. Dist. LEXIS 179858, at *1 (S.D. Ala. Oct. 19, 2018).
[18] *Id.* at *2.
[19] *Id.* at *4.
[20] *Id.*
[21] *Id.* at *5-6.
[22] *Id.* at *8.

not evident from the record—appeared to deal with video material where the person being videotaped did not know, at least initially, that they were being recorded.[23] The court distinguished those citations noting the corporate designee here received notice of the video deposition to be utilized in domestic civil litigation.[24] Finally, court noted the absence of any applicable foreign law proscribing the videotaping under the circumstances, and therefore allowed the videotaping under the condition the videotaped component of the deposition (as opposed to the written deposition transcript) not be publicly disclosed or utilized in any other investigation or litigation.[25]

Considering the type of deposition involved and the rights of the data subject, more may be implicated than the court directly addressed. The witness presumably agreed to be designated as the Rule 30(b)(6) witness when the deposition was first noticed without stating the recordation means. After the deposition notice was amended to reflect video recording, the witness objected. The noticing party, thus, altered the situation from one with consent of the witness to one where the witness' agreement to the video became an issue.

Article 6 of the GDPR requires, above all, that data processing be lawful, and offers numerous bases for lawful processing. The first ground of lawful processing is consent of the subject.[26] In the context of video depositions, however, the personal data objected to by the data subject will not exist until the deposition is recorded. The other bases for lawful processing under Article 6.1 do not obviously apply to data to be *created* in litigation because they address data already in hand, and in the litigation situation, the Controller whose processing is at issue is not apparent.[27] If the party noticing the deposition is the Controller, it is difficult to see how it may compel a specific 30(b)(6) designee to give permission for videotaping. If the party responding to the deposition notice (the witness's employer) is the Controller whose processing is at issue, then the objection of the designated witness to a videotaped deposition could cause the party problems in complying with the corporate deposition notice, that is, by proceeding with the objecting witness as its designee. Whether an employer may compel an employee data subject to consent to giving new data (videotaped images) to a third party for the employer's business litigation purposes is not obviously answered by the GDPR.

[23] *Id.* at *11-12.
[24] *Id.*
[25] *Id.* at *12.
[26] GDPR, *supra* note 1, at Article 6.1(a).
[27] *Id*. at Article 6.1(b-f).

The noticed entity may have to find another designee who does not object to the videotaping of his or her deposition.

It is difficult, however, to see how the noticed corporation's problems with its designee would be viewed by the noticing party or a United States court as a basis to quash the Rule 30(b)(6) notice. In either event, citation by the responding party of EU enforcement actions which focus on whether or not private videotaping of the public by a business is too broad and thus outside the posted notice, or inadequately noticed, seems rather inapt where the witness, having received notice, objects to the creation of new data.

Apart from power over the witness's employer (i.e. the corporate party subject to the 30(b)(6) notice), a United States court would appear to have little leverage over the individual EU witness standing on GDPR Article 6.1(a). An EU data subject's additional rights under the GDPR to object to processing may practically compel taking a transcribed-only versus video-recorded deposition.[28] Without the data subject's employer to coerce a compelled witness's objection to a video deposition would appear to have legs. By appearing to disregard the individual consent principle of the GDPR, the *d'Amico Dry* court may have distinguished it on an inconsequential basis.

On the other hand, the GDPR allows legislative adjustment of the data subject's rights where court processes are concerned.[29] This concession to the imperative of judicial independence and the importance of civil proceedings could induce a court to conclude, absent legislation, that imposing conditions limiting the use of the video component of the deposition to the case and forbidding any public disclosure may indirectly, but effectively, satisfy the spirit of the GDPR by protecting the witness subject's data. It is not clear from *d'Amico Dry* whether GDPR Article 23 was considered by the court when it fashioned its conditions on the personal data. Regardless, the limitations imposed by the court do not address the tension between the employer and the witness, because it was not an employer disclosing the employee's personal data, rather, the subject himself, compelled to do so in the service of his employer's litigation interests.

***Corel Software, LLC v. Microsoft*.** In the fall of 2018, the United States District Court for the District of Utah addressed a dispute between Microsoft Corp. and Corel Software LLC. This infringement case involved a request for protective order by Microsoft, and a

[28] *See, for example, id*. at Articles 6, 13, 15-21, 23.

[29] *Id*. at Article 23.1 (f) and (j).

motion to compel discovery by Corel against Microsoft.[30] At issue in the case was "telemetry" data sought from Microsoft which involved a "Live Preview" feature used by Microsoft.[31] Microsoft asserted burdensomeness, undue expense, cumulativeness and dispro-portionality arguments under Rule 26 to resist Corel's requests.[32] The only reference to the GDPR was in the court's description of Microsoft's arguments.[33] Microsoft argued its duties to anonymize retained data sought by Corel created a tension for it under the GDPR, and added to its undue burden and expense in complying with Corel's requests.[34] Microsoft apparently took its duties under the GDPR as to the data as given and did not argue that the GDPR forbade or prevented production of the data, rather it simply made production more expensive.[35]

The court provided no further analysis of this aspect of Microsoft's argument or the GDPR. Instead, the dispute was decided under a standard Rule 26 analysis. The court was not persuaded by Microsoft's burden and undue cost claims and found the requested telemetry data relevant, not cumulative, and the costs not undue.[36] There was no discussion of the need for encryption or anonymization of the data. The court did not discuss in any detail Corel's argument that Microsoft failed to support its cost and disproportionality arguments with evidence of those costs (e.g., anonymizing the retained telemetry data covered by the GDPR); however, it appears from the court's ruling that Corel's argument on this point was well taken.

In re Hansainvest Hanseatische Investment-GmbH. The dispute in *In re Hansainvest Hanseatische Investment-GmbH*[37] arose out of a 28 U.S.C. § 1782 request by a German entity for United States based discovery to be used in a foreign proceeding. After examining the three statutory prerequisites for relief under the statute, and finding the request proper, the court analyzed the discretionary factors affecting application of the statute. The GDPR came up in the discussion of the "burdensomeness" factor, as the United States targets objected that, as some of their data custodians were located outside the United States, the combination of logistics and foreign privacy laws created

[30] No. 2:15-cv-00528-JNP-PMW, 2018 U.S. Dist. LEXIS 172875, at *1 (D. Utah October 5, 2018).
[31] *Id.* at *3.
[32] *Id.*
[33] *Id.* at *3-4.
[34] *Id.*
[35] *Id.*
[36] *Id.*
[37] 364 F. Supp.3d 243 (S.D.N.Y. 2018).

major problems.[38] The court never addressed the extent of proof provided by the respondents concerning the difficulty and costs triggered by the discovery requests to their foreign data custodians. This argument of the United States discovery target with EU data custodians raised the interesting situation of a United States entity against whom discovery was sought under §1782 arguing the GDPR for relief as to the GDPR-data subject aspects of its response to the German plaintiff. One might wonder why a German plaintiff, pursuing foreign litigation, subject itself to the GDPR, would not seek discovery of EU custodians directly through EU processes, rather than through 28 U.S.C. § 1782. While not clear from the opinion, there may well have been a lack discovery tools in the EU and the absence of a pending case in Europe when the §1782 requests were made.

In its analysis, the court cited the Second Circuit's admonition to follow ordinary Rule 26 processes in analyzing burdensomeness and cost objections and, where concerns exist over court involvement in foreign litigation, to err on the side of penning detailed discovery orders versus simply denying requests.[39] Having found the requisites for application, the court granted the discovery application as to the target's domestic custodians without condition. As to the foreign custodians, the court granted the application only to the extent that the applicants (1) assumed the costs of the document production, including the costs of compliance with the GDPR or other applicable European data privacy laws and (2) indemnify the United States entity against any potential breaches of European data privacy laws.[40]

On its face, subpart 1 of the Order appears to be a standard cost-shifting provision to address the objections of the United States entities with foreign data custodians; however, the terms imposed by the court make it a fair question whether or not production under that aspect of the Order will ever occur. Under subpart 1 of the Order, the requesting party is required to pay for the costs of the production, which is defined to include the costs of complying with the GDPR. The Order does not discuss the projected costs—including the details of GDPR compliance—raised by the respondents as to their foreign data custodians, so the predicted cost of producing the data is unknown. The court tellingly characterized the likely cost of the discovery as "significant." Given the size of the data, the difficulty of the logistics, and the pervasiveness of the GDPR requirements, further litigation may well arise when petitioner gets the bill for production.

---

[38] *Id.* at 251-252.
[39] *Id.*
[40] *Id.* at 252.

Perhaps more noteworthy is the superficially innocuous language of subpart 2 of the Order, which requires the requesting party to "indemnify Respondents against any foreign data privacy law breaches." Considering the range and scope of penalties assessable by the responsible governmental authority for breach of the GDPR under Chapter 8, Article 83, the requesting party could determine that the likely benefit of the data to be produced by the respondent's foreign custodians is outweighed by the risk of indemnity. This is especially so if the foreign custodians are otherwise amenable to EU process where they are located for production of the data directly, and not circuitously through §1782, which under the court's terms requires indemnification of GDPR breach risk. At the very least it could result in a negotiated reduction in the scope of the data sought.

Uniloc 2017 LLC v. Microsoft. The first 2019 case involving the GDPR comes from the District Court for the Central District of California. In *Uniloc 2017 LLC v. Microsoft Corp.*,[41] the court entered a stipulated protective order referencing the GDPR. The Order contains a paragraph expressly defining "Protected Data" for purposes of the Order:

> 6.1 Protected Data. "Protected Data": refers to any information that a party or non-party reasonably believes to be subject to federal, state or foreign Data Protection Laws or other privacy obligations. Protected Data constitutes highly sensitive materials requiring special protection. Examples of such Data Protection Laws include, without limitation, The Gramm-Leach- Biley Act, 15 U.S.C. § 6801 et seq. (financial information); The Health Insurance Portability and Accountability Act ("HIPAA") and the regulations thereunder, 45 CFR Part 160 and Subparts A and E of Part 164 (medical information); Regulation (EU) 2016/679 Of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, also known as the General Data Protection Regulation ("GDPR")."[42]

[41] No. 8:18-CV-020530-AG, 2019 U.S. Dist. LEXIS 20933, at *1 (C.D. Cal. Feb. 5, 2019).

[42] *Id.* at *15.

In paragraph 6.3 of the Order, the parties agreed "productions of Protected Data Information may require additional safeguards pursuant to Federal, State, or foreign statutes, regulations or privacy obligations and will meet and confer to implement these safeguards if and when needed."[43] No specific portions of the GDPR are addressed in the Order, and no specific "additional safeguards" necessitated by GDPR are recited.

Finjan, Inc. v. Zscaler, Inc. Later that month, another California court issued its opinion in *Finjan, Inc. v. Zscaler, Inc.*[44] The lawsuit involved allegations of patent infringement by Zscaler, a U.S. company, brought by the owner of the patents.[45] The discovery at issue sought emails of a United Kingdom citizen, Mr. Warner, who formerly worked for plaintiff and successive licensees of the patents.[46] Zscaler objected to the discovery, claiming production of the emails as requested would cause it to violate the GDPR, and that anonymization and redaction were needed to prevent divulging the personal data of other EU data subjects.[47] Zscaler asked that plaintiff be required to share the costs of compliance, and to defer the United Kingdom email discovery until after domestic production occurred.[48] The plaintiff argued the GDPR was satisfied by less costly means, e.g., designation of the requested foreign emails as attorney-eyes-only under the existing Protective Order.[49] In analyzing the plaintiff's discovery request, the court addressed three fundamental questions in detail. First, the court addressed the authority of United States courts to order discovery where compliance will result in violation by the producing party of a foreign law.[50] Next, the court discussed the factors for consideration when addressing an apparent conflict between foreign law and United States discovery law.[51] Finally, the court discussed whether the GDPR presented a conflict in this case.[52]

Of the eleven cases reviewed, this opinion provides the most thorough analysis of the role of foreign requirements in the discovery process in U.S. litigation. The court's discussion will likely prove a model for analysis by future courts called upon to address these issues.

Although the court evaluated the factors and concluded they weighed in favor of production of

---

[43] *Id.* at *16.
[44] No. 17-cv-06946-JST (KAW), 2019 U.S. Dist. LEXIS 24570, at *1 (N.D. Cal. Feb. 14, 2019).
[45] *Id.* at *2.
[46] *Id.*
[47] *Id.* at *3.
[48] *Id.*
[49] *Id.*
[50] *Id.* at *4.
[51] *Id.*
[52] *Id.* at *6.

the requested discovery, the court ruled based on its finding that the GDPR did not preclude production of the requested data in an un-redacted form under the existing Protective Order.[53] Problems for the objecting defendant included its concession that the GDPR did not preclude production of personal data objectively related to the subject of the litigation, and its failure to present evidence of the extent of the burden to support its cumulativeness argument and request for a staged production. Similarly, based on the court's analysis, it is not apparent the defendant had a good explanation as to why the limited search terms proposed by the plaintiff were too broad, or how production of the emails discussing plaintiff's patent—without the names of email recipients—were not objectively related to plaintiff's claim of patent infringement.

United States Soccer Federation v. Silva International Investments. In May 2019, a District Court in Florida addressed a dispute regarding subpoenas. In *United States Soccer Federation, Inc. v. Silva International Investments*,[54] the plaintiff issued subpoenas to be enforced by the United States District Court in Florida. In contesting the subpoenas, the defendant argued the breadth of the requests subjected it to risks of massive fines under the GDPR for disclosing personal data of EU citizens and the expenses of complying with the subpoena would cause undue hardship and expense.[55] The defendant also asked for indemnification by the plaintiff for any liability that may arise under the GDPR.[56] Finding the motion raised complex issues, including the scope and proportionality of the discovery, jurisdiction over a United Kingdom company, the effect of the GDPR on United States ordered discovery, as well as comity issues, cost-shifting, and indemnification, the magistrate judge recommended that the case be transferred under Rule 45 to the United States District Court which originally issued the subpoena.[57]

Morgan Art Foundation Ltd. v. McKenzie. In the final case to be discussed, the Southern District of New York addressed a plaintiff's general objection to discovery characterized by the defense as evincing an obstructive intent. In *Morgan Art Foundation Ltd. v. McKenzie*,[58] the plaintiff raised the GDPR and Swiss privacy laws in

[53] *Id.* at *11.
[54] No. 19-21119-MC-Cooke/Goodman, 2019 U.S. Dist. LEXIS 75350, at *1 (S.D. Fla. May 2, 2019).
[55] *Id.* at *6.
[56] *Id.*
[57] *Id.* at *10.
[58] No. 18 Civ. 4438 (AT), 2019 U.S. Dist. LEXIS 109997, at *1 (S.D.N.Y. July 1, 2019).

general objections to discovery propounded by the defendant. In its objections, plaintiff stated it would produce documents "only in accordance with, and upon and after complying with, all applicable laws, statutes and regulations."[59] The raising of this general objection was argued by the defendant as evidence of the plaintiff's intention to avoid and evade discovery in connection with a request for stay of the action and imposition of a bond as condition of the stay.[60] As such, the issue of production of specific items subject to specific provisions of the GDPR or laws of Switzerland was not yet before the court.[61] The court disagreed with the significance of the general objection, noting it would "not penalize the Plaintiff for complying with the laws of the jurisdictions in which it operates."[62]

III. Conclusion

As a general principle, the court's sentiment in *Morgan Art Foundation* will most likely be applicable across courts. No court has categorically rejected issues raised under GDPR, and no court has given a responding party a pass merely for citing it. Court orders have reflected empathy toward GDPR-based data privacy concerns, whether or not couched as such. Litigants seeking to effectively utilize the GDPR as a bar or as a means to limit discovery must, however, be precise in their objections and thorough in demonstrating their burdens and costs if they hope to fit these factors into the court's Rule 26 analysis. This is no different than the burden on litigants with any other basis for objection under the rule.

---

[59] *Id.* at *13.
[60] *Id.*
[61] *Id.*
[62] *Id.*