GUIDELINES FOR GDPR COMPLIANCE IN THE CONTEXT OF US LITIGATION DISCOVERY AND INVESTIGATION

General Data Protection Regulation Team, Published March 2024

TABLE OF CONTENTS

Checklist Guidelines For GDPR Compliance

1. Have reasonable attempts been made to avoid discovery/disclosure that includes Personal Data of European Economic Area ("EEA") and the United Kingdom ("UK") Data Subjects?
    - Resolving the dispute without the need for discovery
    - Looking for other substitute sources of information either outside of Europe or outside of the organization entirely

2. Have reasonable attempts been made to minimize the volume of records containing Personal Data covered by the GDPR that is subject to potential review and production?
    - Pushing back on overbroad requests—what is really necessary to resolve disputed issues in the litigation?
    - Considering the sensitivity of the data in view of the risks and impact to the individuals involved
    - Limiting the number of custodians, especially where they are likely to have duplicative information
    - Limiting the data sources for each custodian to what is necessary and non-duplicative
    - Using date limiters, key words, deduplicating, and analytics to limit the amount of data collected from each custodian

3. Has phased discovery been considered (e.g. by custodian, time period, or preliminary case issues)?

4. Has a lawful basis for processing the data been identified and documented?

5. Has appropriate notice been provided to EEA/UK Data Subjects whose Personal Data is implicated?

6. Has the possibility of conducting in-country review been considered to further narrow the document population prior to any cross-border transfer?
    - Even if it is impractical to conduct review fully in-country, can data be minimized in the EEA/UK prior to review in, or transfer of the data to, the U.S. to weed out unnecessary information?
    - Even if it is impractical to conduct in-EEA/UK review, can the data be hosted in the EU/UK during the review to reduce the risk of data breaches in the U.S.?

7. Has there been exploration of the potential to redact, anonymize, or pseudonymize Personal Data that is not necessary for the litigation?

8. Have appropriate technical and organizational measures been taken to assure that everywhere the data is hosted or otherwise maintained, and in all transfer steps, the data is protected?

9. Have Service Providers (including law firms and third parties) been vetted and, if appropriate, have receiving parties that are involved in processing, transferring, receiving, and hosting the data been required to provide sufficient guarantees that they are implementing appropriate technical and organizational measures to meet the requirements of the GDPR and ensure the protection of the rights of Data Subjects?

10. Have GDPR-compliant written agreements been executed with every discovery vendor/ service provider?

    - Setting out the subject matter and duration of the processing, the nature and purpose of the processing, the type of Personal Data and categories of Data Subjects, and the obligations and rights of the Controller;
    - Providing that the data will not be transferred or otherwise processed except on documented instructions from the client;
    - Providing that everyone involved in the transfer or other processing is required to protect the confidentiality of the personal information, and implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk;
    - Requiring assistance in complying with GDPR obligations;
    - Requiring that the vendor or service provider deletes or returns all Personal Data, at the client's request, at the end of the provision of services, and at other appropriate times throughout the process;
    - Immediately notifying the client of any data security incidents;
    - Providing that the vendor or service provider will make available sufficient information to demonstrate compliance with GDPR obligations and will cooperate with any audit or investigation; and
    - Requiring that the vendor or service provider not rely on any other sub-vendors or service providers without advance written consent, and their separate execution of an acceptable agreement that includes all of the above terms.

11. Can arrangements be made for production "in place" (ideally in the EEA/UK, but otherwise still in the control of the producing party) rather than transferring data to requesting parties? Access from a remote location is considered to be both processing and transfer in the location from which the data is accessed. However, remote access, as opposed to direct transfer of data, along with other steps identified on this checklist and in the accompanying guidelines, can still be part of a program to maximize protection of the data.

12. If production cannot occur in the EEA/UK, has there been documentation of a lawful basis for transferring the data to the U.S.?

    - E.g., that the transfer is necessary for the establishment, exercise, or defense of legal claims as provided under Article 49?; OR
    - The transfer is not repetitive, concerns only a limited number of Data Subjects, is necessary for the purposes of compelling legitimate interests pursued by the Controller which are not overridden by the interests or rights and freedoms of the Data Subject, and the controller has assessed all the circumstances surrounding the data transfer and has provided suitable safeguards in regard to the protection of Personal Data. The controller must also inform the supervisory authority and the Data Subject of the transfer and the compelling legitimate interest pursued.

13. Does any of the data in question contain Personal Data of a child requiring additional protection or any special categories of Personal Data under Article 9 (information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, the processing of genetic or biometric data, health data, or data concerning individuals' sex lives or sexual orientation) or criminal records? If so, have additional steps been taken to protect it?

14. Has a protective order been obtained in the litigation to implement data protection measures, including requiring:

    - The minimization of data before transfer or production, including elimination of any data not necessary for the establishment, exercise, or defense of legal claims or defenses;
    - De-identification or "pseudonymization" (within the meaning of the GDPR) of data subjects before transfer or production to the extent practical and appropriate;
    - Consideration of sending a person to a third country to assess, before any transfer, the relevance of data to a particular matter;
    - Access on a needs-only basis and use only as required for the establishment, exercise, or defense of legal claims or defenses;
    - All recipients of the Personal Data to take adequate technical and organizational measures to protect the Personal Data;

- The producing party and the court must immediately be notified in the event of a government request or demand for that data or a data security incident involving data that has been produced, and that the parties comply with resulting legal obligations;
- Parties to the litigation not to provide access to any experts, consultants, or other third parties without a litigation need, adequate advance notice to the producing party, an opportunity for the producing party to object, and agreement by the recipient(s) to be bound by the terms of the protective order;
- The redaction of Personal Data before any court filing or, where appropriate, filings under seal;
- Providing for the return or destruction of all data, including Personal Data, as soon as it is no longer necessary for the litigation;
- That Data Subjects whose personal information is included in any transfer will be given access and standing to raise with the court, on a confidential basis, any alleged or potential violation of their rights; and
- That all documents containing Personal Data subject to the GDPR or other privacy protections be appropriately marked?

Guidelines For GDPR[1] Compliance In The Context Of US Litigation Discovery And Investigations

1. **Have reasonable attempts been made to avoid discovery/disclosure that includes Personal Data of European Economic Area ("EEA") and the United Kingdom ("UK") Data Subjects?**
    - **Resolving the dispute without the need for discovery**
    - **Looking for other substitute sources of information either outside of Europe or outside of the organization entirely**

Reasonable Efforts To Avoid Personal Data Processing

In litigation discovery, the General Data Protection Regulation ("GDPR") must be considered when Personal Data[2] of Data Subjects[3] that is subject to the GDPR[4] is sought or may be produced to a third party to exercise or defend legal claims in the U.S.[5] Due to the difficulties and complexities involved in lawfully processing[6] personal data for U.S. discovery, as discussed in more detail below, reasonable attempts should be made to avoid or limit discovery or disclosure of Personal Data of subjects in the EEA or the UK.[7] Such attempts may include seeking to resolve the dispute without the need for discovery. If dispute resolution prior to discovery is not practical, a party should seek data from an alternate source that is not subject to the GDPR wherever that is a practical alternative.[8]

---

[1] The European General Protection Data Regulation became effective in EEA May 25, 2018. Following the UK's separation from the EU, the UK adopted an essentially identical GDPR, effective January 1, 2021. Except as otherwise specified within these Guidelines, "GDPR" will be used to refer to both the European and UK GDPR.

[2] Article 4(1) of the GDPR broadly defines "Personal Data" to include "any information relating to [a data subject]…such as a name, an identification number, location data, and online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that [data subject]".

[3] Article 4(1) of the GDPR broadly defines "data subject" to include "identified or identifiable natural person…who can be identified, directly or indirectly, in particular by reference to an identifier" such as those listed in note 1 above. See also GDPR Recital 27 which further clarifies that this applies to living persons.

[4] Article 3 of the GDPR identifies the territorial scope of the GDPR.

[5] Article 3 of the GDPR defines its territorial scope to cover the processing of personal data by a controller or processor located in the EEA/UK; or extraterritorially to controllers or processors (a) offering of goods or services to data subjects in the EEA/UK, or (b) monitoring their behavior as far as it takes place in the EEA/UK, regardless of where the processing occurs.

[6] Article 4(2) of the GDPR defines "processing" to include "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

[7] The EEA includes countries in the EU (Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, and Sweden) plus Iceland, Liechtenstein, and Norway. The UK has a parallel statute that tracks the GDPR and applies in England, Northern Ireland, Scotland, and Wales (the UK General Data Protection Regulation and the UK Data Protection Act 2018 that supplements it). Switzerland has separate data protection laws that should also be considered.

[8] Recital 39 of the GDPR provides that "Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means…".

2. **Have reasonable attempts been made to minimize the volume of records containing Personal Data covered by the GDPR that is subject to potential review and production?**

   - Pushing back on overbroad requests—what is really necessary to resolve disputed issues in the litigation?
   - Considering the sensitivity of the data in view of the risks and impact to the individuals involved
   - Limiting the number of custodians, especially where they are likely to have duplicative information
   - Limiting the data sources for each custodian to what is necessary and non-duplicative
   - Using date limiters, key words, deduplicating, and analytics to limit the amount of data collected from each custodian

   If obtaining data from sources outside of the EEA/UK is not a viable alternative to discovery or disclosure of Personal Data, the producing party must make reasonable attempts to minimize the volume of documents containing Personal Data for review, production, and transfer to the U.S. Pursuant to the GDPR, the Personal Data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed ("data minimization")[9]. The following is a non-exhaustive list of how data may be minimized.

   2.1 **Objecting to, or negotiating narrowing of overbroad requests—limit to what is necessary for the establishment, exercise of defense of legal claims:** Overbroad data requests should be refused on the basis that the request is likely to result in the collection, review, production and transfer to the U.S. or personal data which is not relevant or necessary for the establishment, exercise, or defense of legal claims in the U.S. Where the Article 49(1)(e) derogation is being relied upon, a valid argument can also be made that an overbroad request would fall foul of the necessity requirement under Article 49(1)(e)[10].

   2.2 **Considering the sensitivity of the Personal Data in view of the risks and impact to the individuals involved:** During the course of legal proceedings and the collection of Personal Data through legal discovery, certain sensitive data classified as "special category" data or criminal records data under the GDPR may be involved. Because the processing of Personal Data that falls within these "special categories" or criminal records data can present an increased risk to the rights and freedoms of individuals, data minimization efforts should address and mitigate any increased risk. For instance, when collecting data, consider using filters to exclude irrelevant sensitive data. Data analytics and/or keyword search terms should be used to further cull sensitive data and segregate

[9] Article 5(1)(c) of the GDPR.

[10] Article 49(1)(e) of the GDPR provides that in the absence of an adequacy decision or of appropriate safeguards, personal data can be transferred to a third country or international organization where *"the transfer is necessary for the establishment, exercise or defence of legal claims"*.

sensitive but relevant data for separate consideration, including the potential application of redactions, anonymization, or pseudonymization of Personal Data which are addressed at item 7 below. Please note the processing of such sensitive data will require special authorization from individuals or by EEA/UK laws (see Article 9 and 10 GDPR).

2.3 **Limiting the number of custodians, especially where they are likely to have duplicative information:** A party should limit the number of custodians from whom discovery will be collected and/or produced to only those who may possess or control data that is relevant and necessary to the matter. Reasonable efforts should be made to establish the relevancy of each custodian and the data they hold by, for example, preparing a data inventory, circulating a custodian questionnaire, conducting custodian interviews, and asking the requesting party for a justification for inclusion of the custodians, with the aim of reducing the volume of Personal Data collected and ultimately produced.

2.4 **Limiting the data sources for each custodian to what is necessary and non-duplicative:** In addition to limiting the number of relevant custodians, the data sources should be limited for each custodian. The preparation of a data inventory, completion of custodian questionnaires, and follow up interviews will assist with identifying truly necessary data sources. Parties should avoid being overinclusive when identifying data sources.

2.5 **Limiting the file and data types collected to types that are likely to include relevant data:** The collecting party (e.g., counsel, eDiscovery consultant, internal eDiscovery team) should become familiar with the organization's data before agreeing to the scope of production. Certain file and data types may be more likely to contain significant volumes of Personal Data, or unlikely to have any relevant information, and attempts should be made to agree that those file types can be excluded from the production.

2.6 **Using date limiters, keywords, de-duplication, and analytics to limit the amount of data collected from each custodian:** Once the relevant custodians and data sources have been identified, search terms, date limiters, and/or keywords should be considered to filter and exclude from production certain information that is not relevant or necessary, and/or include for potential production only relevant and necessary data, thereby limiting the volume of data collected. The data should also be de-duplicated to further reduce the volume of documents. Data analytics such as email threading, concept clustering, communications analytics, and/or sentiment analysis can also be used to further cull the volume of documents for review and/or to identify a pool or pools of irrelevant data (for exclusion) or potentially relevant data (for inclusion).

3. **Has phased discovery been considered (e.g. by custodian, time period, or preliminary case issues)?**

   Parties to U.S. litigation may protest that the scope of information included in discovery is overinclusive and disproportionate to the needs of the case, resulting in significant costs and delay. Phased discovery may be useful to help achieve proportionality and avoid unnecessary disclosure, with the potential to reduce the need for Processing or transfer of Personal Data unless or until absolutely necessary.

   The implementation of phased discovery involves adopting a staged approach whereby certain parameters (e.g. custodians, date ranges, or data sources) are prioritized and others (typically those less likely to be relevant) are saved for subsequent phases if needed. Phased discovery can allow the parties to focus on the key preliminary issues and potentially narrow the scope of the disputed issues early in the case. In order to streamline the discovery process, the parties might, for example, agree to begin with a phase of discovery focused on a single facet of the case, the resolution of which could be key to the outcome of the litigation (e.g., jurisdictional or statute of limitations issues). In such an instance, they would typically agree to engage in broader discovery only if the case is not resolved or narrowed upon completion of the first phase. The scope of discovery will then become incrementally broader in scope during each phase, upon a showing that the additional discovery is necessary. This approach is most effective when the requesting and producing parties cooperate and work together to identify the key issues, custodians, date limiters, and timing of production.

   It is important to avoid processes that will merely duplicate efforts, which would increase costs and prolong discovery. Actions, such as collection and review, should only be performed once on any particular data set. Adding custodians and document sources at a later time may increase the ultimate cost if there is repetition of the same task for additional documents. Re-collection or re-review of documents from the same sources due to later-added categories, issues, or keywords may be inefficient and should be avoided through careful advance planning.

4. **Has a lawful basis for processing the data been identified and documented?**

Prior to processing Personal Data, the most applicable lawful basis or bases for such Processing should be identified, and litigants should avoid alternating between legal bases. The GDPR identifies six possible bases for lawfully processing Personal Data[11], but the one most likely to apply to cross-border discovery for U.S.-based litigation[12] is the pursuit of legitimate interests[13].

Processing under Article 6(1)(f) can apply to broad categories of data as long as the legitimate interests requiring the processing are not outweighed by the "interests or fundamental rights and freedoms of the data subject…" The three-step test to determine how to incorporate the key elements of 6(f)(1) includes:

1. Purpose Test – is there a legitimate interest behind the processing?
2. Necessity Test – is the processing necessary for that purpose?
3. Balancing Test – is the legitimate interest overridden by the individual's interests, rights, or freedoms?[14]

Before Processing, a legitimate interest analysis (including the lawful basis for processing and, if appropriate, the legitimate interests analysis, conclusions, and any data protection measures implemented to address risks to data subjects' interests, rights, or freedoms) should be conducted and the analysis and conclusions should be documented before Processing to demonstrate compliance with this requirement.

---

[11] Article 6(1) of the GDPR provides: "Processing shall be lawful only if and to the extent if at least one of the following applies:
(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes ;
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for compliance with a legal obligation to which the controller is subject ;
(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

[12] On initial analysis, it might appear that litigant could rely on basis (c) above because the processing is necessary for a party's compliance with their legal obligations under U.S. discovery rules. However, the drafters of the GDPR have made clear that Article 6(1)(c) "legal obligation" language only applies to legal obligations arising under EU law and does not extend to U.S. discovery obligations.

[13] Another potential basis could be Data Subject consent, but that is fraught with additional concerns. For example, the GDPR requires that consent be freely given without coercion and that consent may be withdrawn at any time for any reason. Employee consent at the request of an employer is deemed to be questionable due to the inherent power disparity in any employment relationship, and in the context of litigation discovery the withdrawal of consent is typically impractical.

[14] See https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/.

5. **Has appropriate notice been provided to EEA/UK Data Subjects whose Personal Data is implicated?**

   The GDPR requires transparency regarding the collection, processing and transfer of data so that individuals in the EEA or the UK may exercise their right to the protection of their Personal Data.

Notice regarding collection of data

Where Personal Data is obtained directly from an individual (Article 13), that person must be informed of certain information at the time that the data is obtained, including: the purposes of the Processing for which the Personal Data are intended as well as the legal basis for the Processing;

I. The legitimate interests pursued by the entity that is controlling the collection, processing and/or transfer of the data or by a third party, if that is the basis for lawful processing of the data;

II. The recipients or categories of recipients of the Personal Data, if any;

III. Where applicable, the fact that the Controller intends to transfer Personal Data to a third country or international organization and the existence or absence of an adequacy decision by the European Commission or the UK Information Commissioner or, if transfer is based on some other basis, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available;

IV. The period for which the Personal Data will be stored or, if that is not possible, the criteria used to determine that period;

V. The existence of the right to request from the Controller access to and rectification or erasure of Personal Data or restriction of Processing concerning the Data Subject or to object to Processing as well as the right to data portability;

VI. Where the Processing is based on consent of the Data Subject, their right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

VII. The right to lodge a complaint with a supervisory authority;

VIII. Whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the Data Subject is obligated to provide the Personal Data and of the possible consequences of failure to provide such data;

IX. The existence of automated decision-making, including automated data analytics that may be used on eDiscovery platforms, and, in those cases, meaningful information about the logic involved, as well as anticipated consequences of such Processing on the Data Subject.

If Personal Data is not obtained directly from the Data Subject, he or she must be provided the required information within a reasonable period after obtaining the Personal Data, but at the latest within one month, or if disclosure of the Personal Data is anticipated, at the latest when the Personal Data is first disclosed. The following information should be provided:

I. Identity and the contact details of the entity that is controlling the collection, processing, and/or transfer of the Personal Data and, where applicable, that entity's designated representative in Europe;

II. The contact details of the data protection officer, where applicable;

III. the purposes of the Processing for which the Personal Data are intended as well as the legal basis for the Processing;

IV. The categories of Personal Data concerned;

V. The recipients or categories of recipients of the Personal Data, if any;

VI. Where applicable, the fact that the Controller intends to transfer Personal Data to a third country or international organization and the existence or absence of an adequacy decision by the European Commission or, if transfer is based on some other basis, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available;

VII. The period for which the Personal Data will be stored or, if that is not possible, the criteria used to determine that period;

VIII. The legitimate interests pursued by the entity that is controlling the collection, processing, or transfer of the data or by a third party, if that is the lawful basis for processing the data;

IX. The existence of the right to request access to and rectification or erasure of Personal Data or restriction of Processing concerning the Data Subject and to object to processing as well as the right to obtain a copy of the data in a commonly used, machine-readable, and interoperable format (in most circumstances, free of charge);

X. Where processing is based on the Data Subject's consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

XI. The right to lodge a complaint with a supervisory authority;

XII. The source of the Personal Data and, if applicable, whether it came from publicly accessible sources;

XIII. The existence of automated decision-making, including automated data analytics that may be used on eDiscovery platforms and, in those cases, meaningful information about the logic involved, as well as anticipated consequences of such Processing on the Data Subject.

If the Personal Data is not collected directly from the data subject, and providing the foregoing notice is either impossible or unreasonably expensive, the collection and/or transmission is required by law (foreign law may not be sufficient), or if the data must remain confidential due to obligations to maintain secrecy of processing, compliance with the notice requirements may be excused. This exception applies only to exceptional circumstances.

Children's data (generally below 16 years of age, unless the age threshold is lowered by specific European countries, provided that such age is not below 13 years of age)

The foregoing notices should be provided to a child's legal guardian, if the Personal Data at issue belongs to a child. The entity shall make reasonable efforts to verify that the consent is given or authorized by the child's legal guardian.

Consent

If an entity uses consent as a basis to lawfully process and transfer data, the organization should retain documentation of that consent, sufficient to demonstrate that the data subject or, if a minor, the Data Subject's legal guardian, has consented to such processing and/or transfer of the Personal Data.

6. **Has the possibility of conducting in-country review been considered to further narrow the document population prior to any cross-border transfer?**

   - Even if it is impractical to conduct review, fully in-country, can data be minimized in the EEA/UK prior to review in, or transfer of the data to, the U.S. to weed out unnecessary information?
   - Even if it is impractical to conduct in-EEA/UK review can the data be hosted in the EU/UK during the review to reduce the risk of data breaches in the U.S.?

In-Country Review

The GDPR requires that any transfer of Personal Data to the U.S. be limited to what is "necessary." One of the ways to avoid transferring unnecessary data is to eliminate that data prior to transfer. That can start with some of the technological filtering techniques identified under Item 2, but the data can be further filtered by human review. By conducting the review in the jurisdiction where the data is already located or routinely

lawfully accessed or, if that is not practical, by conducting the review in another jurisdiction deemed to be adequate[15], the amount of Personal Data that must be transferred to the U.S. can be further minimized in accordance with GDPR mandates. Where practical constraints restrict the ability for a full review in-country, some human review, even on a batch or file basis, can help to weed out irrelevant documents. Analytics tools (sometimes referred to as Early Case Assessment ("ECA") or Early Data Assessment ("EDA") tools) can be leveraged by human reviewers to efficiently aid such data minimization efforts.

Where conducting review in-country is not possible or practical, a fallback strategy is to host the data on-line in-country and then review and filter remotely from the U.S. Note that, based on EU interpretations and directives, allowing any access of data from the U.S. is considered Processing and thus a "transfer" to the U.S., regardless of whether the data is hosted, so all other GDPR requirements for transfer must still be met. Nevertheless, to the extent that keeping the data hosted in a country deemed to have adequate privacy protection may add a higher level of data protection, it can reduce the risks that must be balanced against the legitimate interests for Processing and transfer in order to advance GDPR compliance.

7. **Has there been exploration of the potential to redact, anonymize, or pseudonymize Personal Data that is not necessary for the litigation?**

Redaction, anonymization, and pseudonymization measures can be applied in order to give effect to a number of data protection principles arising under the GDPR, including data minimization[16], data protection by design[17], and the principle of integrity and confidentiality[18]. While such measures will likely be applied by the data exporter prior to a transfer being effected, they may be equally relevant to consider in the context of storage of Personal Data and onward transfers of Personal Data, where applicable.

Redaction

Redaction may be used to remove information which is determined as being out of scope following the analysis at Item 2 above. Whether applying manual redaction techniques or using specific redaction software, it is important to ensure that the redaction is effective i.e. that the redaction is permanent. Furthermore, the presence of metadata which may be embedded in a particular file should also be considered.

[15] Here is the list of countries that obtained the European Commission's and the UK Information Commissioner's adequacy decision as of the date of this document: Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, and Uruguay. The Republic of Korea obtained an adequacy decision from the European Commission most recently (not yet recognized by the UK).

[16] Article 5(1)(c) of the GDPR.

[17] Article 25 of the GDPR.

[18] Article 5(1)(f) of the GDPR.

Pseudonymization[19]

Pseudonymization involves replacing the identifying characteristics of Personal Data with a reference or pseudonym, in order to prevent the Data Subject from being identified. Pseudonymized data may be attributed to a natural person by the use of additional information and therefore could constitute Personal Data and remain subject to the data protection requirements under the GDPR. Such additional information should be stored separately and subject to appropriate technical and organizational safeguards. In the case of an EU-U.S. Personal Data transfer, such additional information allowing for re-identification may, for example, be held exclusively by the data exporter.[20]

Anonymization

Anonymized data comprises information which does not relate to an identified or identifiable natural person or Personal Data that has been rendered anonymous in such a way that the Data Subject is no longer identifiable. Data that has been effectively and irreversibly anonymized is no longer considered Personal Data and therefore falls outside the scope of application of the GDPR.[21] Please note that the threshold that must be reached in order for data to be considered "anonymized" is quite high and anonymization may be considered as an alternative to deletion.[22] If there is a reasonable risk that the anonymization can be reversed, the data may be "pseudonymized" data.

8. **Have appropriate technical and organizational measures been taken to assure that everywhere the data is hosted or otherwise maintained, and in all transfer steps, the data is protected?**

   Organizations that host or access information should maintain a cybersecurity program designed to protect the confidentiality, integrity, and availability of information and related systems. This can include:

   - Identifying internal and external cybersecurity risks and conducting a Data Protection Impact Assessment ("DPIA") as may be appropriate;

[19] Article 4(5) of the GDPR: 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

[20] See "Use Case 2: Transfer of pseudonymised Data" on page 23 of the EDPB's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. Here the EDPB sets out the circumstances under which it considers pseudonymization as providing an effective supplementary measure in the context of personal data transfers to outside of the EU.

[21] Recital 26 of the GDPR.

[22] Paragraph 54 of the EDPB's Guidelines 4/2019 on Article 25 Data Protection by Design and by Default.

- Maintaining policies and procedures (e.g., data retention, incident response, disaster recovery, acceptable use, access, BYOD (bring your own device), data minimization, etc.) as may be appropriate;
- Having physical security controls in place;
- Monitoring network activity;
- Considering penetration testing;
- Maintaining compliance records, including cybersecurity audit trails;
- Considering encryption and other data protection measures, such as multi-factor authentication;
- Confirming compliance with security requirements of other laws that may apply in addition to GDPR (such as state laws, HIPAA, GLBA, etc.); and
- Conducting regular training of personnel and enforcing compliance.

9. **Have service providers (including law firms and third parties) been vetted and, if appropriate, have receiving parties that are involved in processing, transferring, receiving, and hosting the data been required to provide sufficient guarantees that they are implementing appropriate technical and organizational measures to meet the requirements of the GDPR and ensure the protection of the rights of Data Subjects?**

   Sufficient guarantees to ensure compliance with the GDPR and protection of the rights of data subjects may include:

   - Identifying all service providers that may access or receive Personal Data;
   - Conducting a security risk assessment (and completing a DPIA, as may be necessary);
   - Considering incorporating security requirements into a protective order, and requiring appropriate service providers to execute an acknowledgment and agreement to be bound by it;
   - Considering the items listed in Item 8 above and applying them to service providers; and
   - Having contracts that cover security issues, deletion of data, maintaining records to demonstrate compliance in line with Article 28, where service providers are Processors, as well as incorporating any applicable confidentiality and/or court protective orders, and including an enforcement mechanism.

10. **Have GDPR-compliant written agreements been executed with every discovery vendor/ service provider?**

    - Setting out the subject matter and duration of the processing, the nature and purpose of the processing, the type of Personal Data and categories of Data Subjects, and the obligations and rights of the Controller;

- Providing that the data will not be transferred or otherwise processed except on documented instructions from the client;
- Providing that everyone involved in the transfer or other processing is required to protect the confidentiality of the personal information, and implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk;
- Requiring assistance in complying with GDPR obligations;
- Requiring that the vendor or service provider deletes or returns all Personal Data, at the client's request, at the end of the provision of services, and at other appropriate times throughout the process;
- Immediately notifying the client of any data security incidents;
- Providing that the vendor or service provider will make available sufficient information to demonstrate compliance with GDPR obligations and will cooperate with any audit or investigation; and
- Requiring that the vendor or service provider not rely on any other sub-vendors or service providers without advance written consent, and their separate execution of an acceptable agreement that includes all of the above terms.

The GDPR requires Controllers to enter into a legally binding contract when a Controller engages a Processor to process Personal Data on its behalf[23]. It is therefore necessary to have a written data processing agreement[24] in place with all e-discovery service providers that will be processing data for GDPR compliance purposes and to avoid GDPR fines.

Article 28 of the GDPR prescribes the provisions which must be included in a data processing agreement between a Controller and a Processor. A data processing agreement must at the very least contain the following details:

- The subject matter, duration, nature, and purpose of the data processing;
- The type of Personal Data being processed;
- The categories of Data Subjects whose Personal Data is being processed; and
- The obligations and rights of the Controller.

A data processing agreement should also contain the following mandatory provisions[25]:

- That the Processor will only process Personal Data received from the Controller on documented instructions of the Controller (unless required by EU/UK law to process Personal Data without such instructions) including in respect of international data transfers;

---

[23] Article 28 of the GDPR covers data processing agreements under Section 3: Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

[24] A data processing agreement is a legally binding contract that states the rights and obligations of each party concerning the protection of Personal Data.

[25] Article 28 Section 3(a)-(h).

- That the Processor ensures that any person(s) processing Personal Data is subject to a duty of confidentiality;
- That the Processor takes all measures required pursuant to Article 32 (Security of Processing) including but not limited to implementing appropriate technical and organizational measures to protect Personal Data received from the Controller;
- That the Processor obtains either a prior specific authorization or general written authorization for any sub-processors the Processor may engage to process the Personal Data received from the Controller. The Processor must further ensure that where a general written authorization to the Processor engaging sub-processors is obtained, the Controller has the opportunity to object in advance to each individual sub-Processor to be appointed by the Processor;
- That any sub-processors engaged by the Processor are subject to the same data protection obligations as the Processor and that the Processor remains directly liable to the Controller for the performance of a sub-processor's data protection obligations;
- That the Processor assists the Controller by appropriate technical and organizational measures to respond to Data Subject rights' requests under the GDPR;
- That the Processor assists the Controller to ensure compliance with obligations under the GDPR in relation to security of data processing (Article 32), notification of data breaches (Articles 33 and 34), and DPIAs (Article 35 and 36);
- That, at the end of the data processing by the Processor and, on the Controller's instruction, the Processor deletes or returns the Personal Data received from the Controller; and
- That the Processor makes available to the Controller all information necessary to demonstrate compliance with Article 28 of the GDPR and that the Processor allows for and contributes to audits conducted by the Controller or a third party on the Controller's behalf.

There are a number of other provisions which Controllers and Processors may wish to include in data processing contracts which are not mandatory for inclusion under the GDPR. Such provisions may include but are not limited to:

- Liability provisions (including indemnities);
- Detailed (technical) security provisions; and/or
- Additional cooperation provisions between the Controller and Processor.

Such additional provisions may be agreed between Controllers and Processors on a case-by-case basis.

11. **Can arrangements be made for production "in place" (ideally in the EEA/UK, but otherwise still in the control of the producing party) rather than transferring data to requesting parties? Access from a remote location is considered to be both Processing and transfer in the location from which the data is accessed. However, remote access, as opposed to direct transfer of data, along with other steps identified in these guidelines, can still be part of a program to maximize protection of the data.**

Arranging for production where the Controller[26] maintains control of the Personal Data should be considered as an option for added protection. Through a review or production "in place," the reviewing or receiving party is granted remote access to the data through the Controller's system instead of receiving a traditional data transfer. This method of processing is an additional measure the controller can take to meet its obligation to provide appropriate security for the Personal Data.[27]

The Controller must appreciate that providing remote access is considered Processing and transfer of the data. Therefore, all necessary steps discussed in these guidelines should still be taken to protect Personal Data.[28] When possible, the Controller should arrange for remote access from within the EEA/UK. By limiting remote access to the EEA/UK, the Controller avoids the burden of managing a third-country data transfer.[29] Remote access from the U.S. is possible; however, remote access from outside the EEA/UK is also deemed a transfer, and must adhere to the same requirements as a traditional third-country data transfer.[30]

12. **If production cannot occur in the EEA/UK, has there been documentation of a lawful basis for transferring the data to the U.S.?**

- E.g., that the transfer is necessary for the establishment, exercise, or defense of legal claims as provided under Article 49?; OR
- The transfer is not repetitive, concerns only a limited number of Data Subjects, is necessary for the purposes of compelling legitimate interests pursued by the Controller which are not overridden by the interests or rights and freedoms of the Data Subject, and the Controller has assessed all the circumstances surrounding the data transfer and has provided suitable safeguards in regard to the protection of Personal Data. The Controller must also inform the supervisory authority, and the Data Subject of the transfer and the compelling legitimate interest pursued.[31]

Effective July 2023, the European Commission adopted an adequacy decision regarding the EU-US Data Privacy Framework (DPF). Those entities participating in the DPF do not need to implement additional safeguards in order for cross-border transfers to the US from the EEA/UK to occur. However, onward transfers often required in litigation discovery still require data protection steps as set forth elsewhere in these Guidelines.

---

[26] Article 4(7) of the GDPR defines 'controller' as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law."

[27] Article 5.1.(f) of the GDPR; See also Article 32 (Security of processing).

[28] Article 4(2) of the GDPR defines 'processing' to include "...disclosure by transmission, dissemination or otherwise making available" the personal data.

[29] See Articles 44-50 of the GDPR.

[30] EDPB FAQ nr. 11 "it should be borne in mind that even providing access to data from a third country, for instance for administration purposes, also amounts to a transfer", EDPB Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, 23 July 2020.

[31] Note that the legitimate interest analysis for data transfers is separate from, and in addition to, the analysis required to justify data processing. See Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR.

In the absence of appropriate safeguards and/or an adequacy decision under Articles 45-46, data transfers outside of the EEA/UK may still be permissible if the transfers are "necessary for the establishment, exercise, or defense of legal claims."[32] "Legal claims" may refer to any proceeding, including pre-trial discovery, criminal, civil, administration, and arbitration proceedings, as long as the relevant proceeding has a basis in law and there is a close link between the data transfer and proceeding. The derogation may be applied to "transfer of data for the purpose of defending oneself or for obtaining a reduction or waiver of a fine legally foreseen." However, transfer of Personal Data cannot be justified in the anticipation of future legal proceedings. Transfers under this provision must still meet the other data protection requirements (data minimization, proportionality, necessity, confidentiality protections, etc.) otherwise set forth in these Guidelines.[33]

For entities that have not taken the steps necessary to participate in the DPF or UK Data Bridge, and if no other transfer tool is available under Articles 45-46, then a derogation may be considered.[34] Amongst these derogations, "a transfer to a third country or an international organization may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of Personal Data. The controller shall inform the supervisory authority of the transfer."[35] Transfer must be justified by the following:

I. The transfer must be necessary for the purpose of pursuing compelling legitimate interests of the data Controller as long as they do not override the interests or rights and freedoms of the Data Subject;

II. The transfer is not repetitive;

III. The transfer concerns only a limited number of Data Subjects. There is no quantitative definition for the "limited number of Data Subjects," and this must be evaluated on a case-by-case basis;

IV. A balancing test is performed between the "compelling legitimate interests of the data Controller" and the "interests or rights and freedoms of the Data Subject(s)."[36] The data exporter must provide suitable safeguards[37] in regards to protecting the transferred data. Appropriate safeguards must be determined on a case-by-case basis, considering the specific data in question;

---

[32] *See* Article 49(1)(g) of the GDPR.

[33] *See* EDPB Guidance at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf.

[34] Transfers within companies may also be based on binding corporate rules pursuant to Article 47 of the GDPR, but that would not cover onward transfers required for litigation.

[35] *See* Article 49(1) § 2 of the GDPR.

[36] The EDPB advises consideration in regards to the rights and freedoms of the data subjects for "any possible damage (physical and material, but also non-material as e.g. relating to a loss of reputation)."

[37] Safeguards may include but are not limited to: "measures aimed at ensuring deletion of the data as soon as possible after the transfer, or limiting the purposes for which the data may be processed following the transfer. Particular attention should be paid to whether it may be sufficient to transfer pseudonymized or encrypted data."

V. As an additional safeguard, the relevant supervisory data authority must be informed of the transfer; and

VI. The Data Subject must be informed of the transfer and the compelling legitimate interest pursued.[38]

VII. You must document the assessment of the above factors as well as additional suitable safeguards identified above. [39]

13. **Does any of the data in question contain Personal Data of a child requiring additional protection or any special categories of Personal Data under Article 9 (information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, the processing of genetic or biometric data, health data or data concerning individuals' sex lives or sexual orientation) or criminal records?[40] If so, have additional steps been taken to protect it?**

A data protection impact assessment, within the meaning of Article 35, should contain at least:

- A systematic description of the envisaged Processing operations and the purposes of the processing, including the legitimate interest pursued by the Controller;
- An assessment of the necessity and proportionality of the Processing operations in relation to the purposes of the Processing;
- An assessment of the risks to the rights and freedoms of Data Subjects;
- The measures envisaged to address the risks identified, including safeguards, security measures, and mechanisms to ensure the protection of Personal Data and to demonstrate compliance with the GDPR, taking into account the rights and legitimate interest of Data Subjects and other persons;
- Minimization of data before transfer or production, including elimination of any data not necessary for the establishment, exercise, or defense of legal claims or defenses;
- De-identification or "pseudonymization" (within the meaning of the GDPR) of Data Subjects before transfer or production to the extent practical and appropriate;
- Encryption of the Personal Data; and
- Limiting access to special categories of Personal Data, children's data, or criminal records data exclusively to those who need it.

[38] *See* Articles 13 and 14 of the GDPR.
[39] See Article 49(6) of the GDPR.
[40] Note that if any data has been collected from video recording devices, consult Guidelines 3/2019 on processing of personal data through video devices.
[41] *See* **Attachment A** for template protective order.

14. **Has a protective order[41] been obtained in the litigation to implement data protection measures?**

- The minimization of data before transfer or production, including elimination of any data not necessary for the establishment, exercise, or defense of legal claims or defenses;
- De-identification or "pseudonymization" (within the meaning of the GDPR) of Data Subjects before transfer or production to the extent practical and appropriate;
- Consideration of sending a person to a third-country to assess before any transfer the relevance of data to a particular matter;
- Access on a needs-only basis and use only as required for the establishment, exercise, or defense of legal claims or defenses;
- All recipients of the Personal Data to take adequate technical and organizational measures to protect the Personal Data;
- The producing party and the court be immediately notified in the event of a government request or demand for that data or a data security incident involving data that has been produced, and that the parties comply with resulting legal obligations;
- Parties to the litigation not to provide access to any experts, consultants, or other third parties without a litigation need, adequate advance notice to the producing party, an opportunity for the producing party to object, and agreement by the recipient(s) to be bound by the terms of the protective order;
- The redaction of Personal Data before any court filing or, where appropriate, filings under seal;
- Providing for the return or destruction of all data, including Personal Data, as soon as it is no longer necessary for the litigation;
- That Data Subjects whose personal information is included in any transfer will be given access and standing to raise with the court, on a confidential basis, any alleged or potential violation of their rights; and
- That all documents containing Personal Data subject to the GDPR or other privacy protections be appropriately marked.

One of the challenges of cross-border transfers for litigation discovery is that the transferred materials do not all remain with the transferee—typically the US law office (and often their US eDiscovery hosting solution provider). Rather, US litigation parties typically face the obligation to produce to opposing parties that information that is relevant to the dispute and non-privileged. Some of that information may also need to be shared with others in the course of the litigation – including deposition witnesses, experts, judges, jurors, and other related personnel such as court reporters and administrators. Moreover, many court records, including filings that contain Personal Data or that attach documents containing Personal Data, are left accessible to the public. These onward transfers, and other disclosures, therefore run contrary to the privacy requirements of the GDPR.

[41] *See* **Attachment A** for template protective order.

Accordingly, U.S. litigation parties dealing with Personal Data of European data subjects should seek to have a suitable protective order signed by the court in order to protect such Personal Data and advance the privacy dictates of the GDPR, Item 14 identifies the provisions that should be included in such a protective order, and a form of protective order that includes these items is attached to these guidelines as Exhibit A.

U.S. litigation parties should object to producing any information or documents subject to the GDPR unless or until a suitable protective order is in place. This can often be accomplished through cooperative negotiations with opposing parties. Where, however, opposing parties refuse to cooperate, the producing party should still seek court intervention to enter such protective order before producing any covered materials.

Appendix A: Template Protective Order

[COURT NAME/JURISDICTION]

In Re: ABC, Plaintiffs, v. XYZ, Defendant.	Case No.: STIPULATED GDPR PROTECTIVE ORDER

I. PURPOSES AND SCOPE

1.1 Discovery in this action includes confidential, proprietary, or private information subject to privacy requirements of the EU General Data Protection Regulation (Regulation (EU) 2016/679) and other analogues, such as the United Kingdom's Data Protection Act 2018 and/or other privacy regulations. For convenience, we will use the short term "GDPR" in this Order, but the intent is to cover all such privacy regulations.

1.2 The parties hereby stipulate to, and petition the Court to enter, this Stipulated Protective Order ("Order"). This Order shall govern the preservation, collection, ingestion, Processing, transfer, hosting, use, and ultimate proper disposal or return of information that includes Personal Data subject to the GDPR, in accordance with the definitions and other provisions below. The obligations imposed by this Order shall remain in effect and shall survive any final judgment or settlement in this Action. The Court shall have continuing jurisdiction over the Parties to this Action for purposes of enforcing the terms and provisions of this Order.

II. DEFINITIONS

2.1 **Action** means the above–captioned litigation and all related proceedings.

2.2 **Data Subject** refers to any natural person who may be directly or indirectly identified through name, any identification number, location data, online identifier or one or more physical, physiological, genetic, mental, economic, cultural or social identifiers specific to that person.

2.3 **Discovery Material** refers to any information or tangible item, regardless of the medium or manner in which it is generated, stored, or maintained, that is Processed, produced, or generated in disclosures or in response to discovery in this Action.

2.4 **Final Disposition** is deemed to be the later of (i) dismissal of all claims and defenses in this Action; or (ii) final judgment herein after the completion and exhaustion of all appeals, hearings, remands, trials, or reviews of this Action, including the time limits for filing any motions or applications for extension of time pursuant to applicable law.

2.5 **Litigation Support Provider** refers to a person or entity that is assisting one or more Parties, or Non-Parties data collection, filtering, ingestion, Processing, Pseudonymisation, hosting, or related services necessary for this Action.

2.6 **Non-Party** refers to any natural person, partnership, corporation, association, or other legal entity not named as a Party to this action.

2.7 **Party** refers to any party to this Action, including all of its officers, directors, employees, consultants, retained experts, service providers, and legal counsel (as well as support staff).

2.8 **Personal Data** refers to any information relating to an identified or identifiable Data Subject.

2.9 **Processing** refers to any operation (or set of operations) performed on Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, dissemination, restriction, erasure or destruction.

2.10 **Producing Party** refers to each Party or Non-Party producing Discovery Material in this Action.

2.11 **Pseudonymisation** refers to processing of Personal Data such that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information (that is kept separately), and encompasses measures to ensure that Personal Data are not attributed to any identified or identifiable natural persons.

2.12 **Receiving Party** refers to the Party receiving Discovery Material from a Producing Party.

2.13 **Signatory** refers to any person who signs any acknowledgment and agreement to be bound by the terms of this Order, including the form contained in Exhibit A to this Order.

2.14 **Special Category Personal Data** refers to personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data (for the purpose of uniquely identifying a natural person), health data or any data concerning a natural person's sex life or sexual orientation.

III. PROTECTION OF DISCOVERY MATERIALS

3.1 **Documents and Data Produced in this Action.** All documents and data compilations produced in this Action that include Personal Data shall be marked "CONFIDENTIAL/PD" and subject to the protections set forth below.

3.2 **Measures to Protect Confidential/PD Information.** All Parties and Non-Parties handling Confidential/PD information shall take appropriate technical and organizational measures to protect and maintain the confidentiality of all such information, appropriate to the data.

3.3 **Notice to Data Subjects.** Any Producing Party that is processing Personal Data must, wherever appropriate (as determined periodically throughout the Action), and as required by the GDPR or other privacy laws, provide notice to all Data Subjects regarding the processing of their Personal Data and their Data Subject rights.[1]

3.4 **Depositions and Written Discovery Responses.** When Personal Data or documents containing Personal Data are used or discussed in a deposition, affidavit, interrogatory response, witness statement, or other written discovery response, all pages reflecting that discussion and the documents themselves shall be designated as "CONFIDENTIAL/PD."

3.5 **Deposition Designations.** For any discussion in a deposition, the court reporter shall label the cover page of the transcript to state that Confidential/PD is contained therein, and shall label as "CONFIDENTIAL/PD" each page of the transcript and/or exhibits to the deposition transcript that contain Confidential Information. Confidential/PD designations of transcripts or portions thereof, also apply to audio, video, or other recordings of the testimony.

[1] *See, e.g.,* Chapter 3 of the GDPR.

IV. CHALLENGING CONFIDENTIAL/PD DESIGNATIONS

4.1 **Challenges to Confidential/PD Designations.** Any Party may challenge a "CONFIDENTIAL/PD" designation if that Party believes that any other Party or Non-Party has designated any documents or data compilations as "CONFIDENTIAL/PD" without valid grounds.

4.2 **Meet and Confer Requirement.** The Challenging Party shall meet and confer with the Designating Party to attempt to resolve such issues and if such efforts are unsuccessful, any Party may seek resolution from the Court. To the extent practical, notice of such dispute, and an opportunity to be heard, shall be provided to any Non-Party or Data Subject whose personal information is implicated by the challenge.

V. USE OF CONFIDENTIAL/PD MATERIAL

5.1 **Basic Principles.** All Confidential/PD information shall be used only for the purpose of this Action. Except as permitted by this Order, the Parties shall not give, show, or otherwise divulge or disclose the Confidential/PD information, or any copies, prints, negatives, or summaries thereof, to any person or entity. As such, the Receiving Party may use Personal Data that is disclosed or produced by another Party or by a Non-Party in connection with this Action only for prosecuting, defending, or attempting to settle this Action. Such Personal Data may be disclosed only to the categories of persons and under the conditions described in this Order, and only as needed to assist in resolving the dispute in this Action, and after weighing the need for disclosure against the privacy rights and interests of the Data Subject(s).

5.2 **Processing of Personal Data.** All Processing of Personal Data must be performed with consideration of the sensitivity of the information, and weighed against the privacy rights of Data Subjects to whom the Personal Data relates. The Parties and Signatories further agree to:

(a) ensure that there is a legitimate basis for Processing the Personal Data;

(b) limit Processing of Personal Data to items necessary for the establishment, exercise, or defense of legal claims or defenses;

(c) make reasonable efforts to avoid excess, duplicative, or unnecessary Processing and use of Personal Data;

(d) in the event that Special Category Personal Data is Processed, redact any Special Category Personal Data that is not necessary for the establishment, exercise or defense of the legal claims at issue; and

(e) implement appropriate technical and organizational measures to protect Personal Data from unauthorized access or use.

5.3 **Data Subjects' Right to Judicial Review.** Data Subjects to whom the Personal Data relates, may raise with the Court (or through other legal channels, foreign or domestic), any alleged or potential violation of their rights under the GDPR and other applicable data protection laws. Such Data Subjects may seek modifications to this Order, or other remedies from the parties or the Court, in furtherance of protecting their privacy rights.

5.4 **Disclosure of "CONFIDENTIAL/PD" Information.** Subject to the other provisions of this order, a Receiving Party may disclose any information or item designated "CONFIDENTIAL/PD" only to:

(a) The Receiving Party's counsel of record in this Action, as well as employees of said counsel of record to whom it is necessary to disclose the information for this Action;

(b) The officers, directors, and employees (including in-house counsel) of the Receiving Party to whom disclosure is necessary for this Action;

(c) Experts, consultants, and service providers retained by the Receiving Party for this action, to whom disclosure is necessary for this Action;

(d) The court and its personnel, as well as court reporters and their staff;

(e) The author or recipient of Discovery Material containing the information or a custodian or other person who otherwise possessed or knew the information; and

(f) During their depositions, witnesses, and attorneys for witnesses, in this Action to whom disclosure is necessary for purposes of this Action.

5.5 **Acknowledgments to be Bound.** Prior to the disclosure of any Confidential/PD information to any person identified in Paragraph 5.4 above (except the Court and its personnel, court reporters, and jurors in this Action), the disclosing Party will provide each potential recipient of Confidential/PD information with a copy of this Order, and obtain a signed acknowledgement, in the form attached to this Order as Exhibit A, confirming that the recipient has read and understood this Order and shall abide by its terms. Such acknowledgements shall be treated as strictly confidential and maintained by counsel for each Party. Only with good cause shown will the acknowledgement be disclosed to any other Party. Persons who come into contact with Confidential/PD information solely for clerical or administrative purposes on behalf of a Party, and who do not retain copies or extracts thereof, are not required to execute acknowledgements but must comply with the terms of this Order.

VI. PERSONAL DATA SUBPOENAED OR ORDERED PRODUCED

6.1 If a Party is served with a subpoena, court order, or other request or demand outside of this Action, that compels disclosure of any information or items designated in this Action as "CONFIDENTIAL/PD," that Party must:

(a) Promptly, and where feasible prior to production, notify in writing the designating Party and the Court. Such notification shall include a copy of the subpoena, order, or other demand;

(b) Promptly, and where feasible prior to production, notify in writing the party who caused the subpoena or order to issue that some or all of the material covered by the subpoena, order, or other request or demand is subject to this Order. Such notification shall include a copy of this Order; and

(c) Take steps, comparable to the steps set forth in this Order, to protect the Personal Data of Data Subjects identified in any materials, transcripts or other data covered by the subpoena, court order, or other demand.

VII. UNAUTHORIZED DISCLOSURE OF PERSONAL DATA

7.1 If a Receiving Party learns that, by inadvertence or otherwise, Personal Data produced to the Receiving Party has been disclosed to any person or in any circumstance not authorized under this Order, the Receiving Party shall immediately: (a) notify in writing the Designating Party of such disclosure, and to whom the material was disclosed; (b) make a reasonable effort to retrieve all unauthorized copies of the Personal Data or materials containing Personal Data and/or confirm disposal of such copies or materials; (c) where practical, inform the person or persons to whom unauthorized disclosures were made, of all the terms of this Order; (d) request such person or persons to execute the "Acknowledgment and Agreement to Be Bound" that is attached hereto as Exhibit A; and (e) notify the Court and notify any relevant supervisory authorities and any other persons who must notified in accordance with the GDPR (including but not limited to Article 33) or other applicable law.

VIII. PROMPT DELETION OF PERSONAL DATA

8.1 When no longer needed for this Action or, at the latest, after final disposition of this Action, the Receiving Party must return or properly dispose of all Personal Data at the Receiving Party's expense, without undue delay. As used in this subdivision, "all Personal Data" includes all copies, abstracts, compilations, summaries, and any other format reproducing or capturing any portion of the Personal Data. The Receiving Party must verify the return or proper disposal of the Personal Data in its possession and in the possession of any of its agents, by executing and transmitting to counsel for the Producing Party an acknowledgement in the form attached hereto as Exhibit B. A copy of each such executed acknowledgement shall be maintained by counsel for the Receiving Party and counsel for the Producing Party.

IX. MISCELLANEOUS

9.1 **Compliance with Discovery Obligations.** This Order does not relieve any party of its obligations to respond to otherwise proper discovery in this Action.

9.2 **Objections and Modifications.** By stipulating to the entry of this Order, no Party waives any right it otherwise would have to object to disclosing or producing any information or item on any ground not addressed in this Order. Similarly, no Party waives any right to seek modification of this Order or to object on any ground to use in evidence any of the material covered by this Order.

9.3 **Violations.** Any violation of this Order may be punished by any and all appropriate measures including, without limitation, injunctions, contempt proceedings and/or monetary sanctions.

IT IS SO STIPULATED, THROUGH COUNSEL OF RECORD.

_____	_____
DATE	ATTORNEYS FOR PLAINTIFF(S)
_____	_____
DATE	ATTORNEYS FOR DEFENDANT(S)

FOR GOOD CAUSE SHOWN, IT IS SO ORDERED.

_____	_____
DATE	UNITED STATES DISTRICT JUDGE
_____	_____
DATE	UNITED STATES MAGISTRATE JUDGE

EXHIBIT A

[insert Case Caption]

ACKNOWLEDGEMENT AND AGREEMENT TO BE BOUND

I, _____ [print or type full name], of _____ [print or type full address], declare under penalty of perjury that I have been given and have read a copy of the Stipulated GDPR Protective Order that was issued by _____ on _____[date] in the case of _____ [fill in case name] (the "Order"). I understand and agree to comply with and to be bound by all the terms of the Order. I understand that Discovery Material disclosed to me is subject to the Order and that I am prohibited from copying, disclosing, or otherwise using such Discovery Material except as provided by the Order. I understand and acknowledge that failure to comply could expose me to sanctions and punishment in the nature of contempt. I solemnly promise that I will not disclose in any manner any information or item that is subject to this Order to any person or entity except in strict compliance with the provisions of this Order. I further agree to submit to the jurisdiction of the Court for the purpose of enforcing the terms of this Order, even if such enforcement proceedings occur after termination of the above-referenced matter. I also understand that my signature on this "Acknowledgement and Agreement to be Bound," indicating my agreement to be bound by the terms of the Order, is required before I may be allowed to receive and review any produced document(s) or material(s) that are designated as "CONFIDENTIAL/PD."

Date: _____

Print Name: _____

Signature: _____

EXHIBIT B

[Insert Case Caption]

ACKNOWLEDGEMENT OF DESTRUCTION OR DELETION OF CONFIDENTIAL/PD INFORMATION

I, _____ [print or type full name], hereby attest and affirm that I am over the age of 18 years and am a resident of _____ County, _____ [list State/Country].

On behalf of _____, I hereby attest and affirm that, as of _____ [date], _____ [Party] has caused to be securely deleted or destroyed, in a manner that prevents recovery or reconstruction, all Confidential/PD information contained in documents, transcripts, and other materials within the scope of the Stipulated GDPR Protective Order that was issued by _____ on _____[date] in the case of _____ [fill in case name]. I declare under penalty of perjury under the laws of _____ [Country] that, to the best of my knowledge, based on my personal knowledge and reasonable investigation, that the above is true and correct.

Date: _____

Print Name: _____

Signature: _____

CONTRIBUTORS

The project team (organizations noted for identification purposes only) includes:

- David Cohen, Partner at Reed Smith, USA (Pittsburgh, PA), Co-Trustee
- Anna Mercado Clark, Partner at Phillips Lytle, USA (New York, NY)
- Wayne Matus, Co-Founder and General Counsel at SafeGuard✓Privacy, USA (Sarasota, FL)
- Chris Bojar, Director of eDiscovery & Litigation Support at Barack Ferrazzano Kirschbaum & Nagelberg, USA (Chicago, IL)
- David Sweetman, Counsel at the Law Library, Ireland (Dublin)
- Ruth McAllister, Senior Associate at McCann Fitzgerald, Ireland (Dublin)
- Tamara Barnes, Health Information Privacy Consultant at Google, USA (Atlanta, GA)
- Jonathan Swerdloff, Director, Global Client Data Services and eDiscovery at Scott & Scott, USA (New York, NY)
- Niamh Murphy, Director of eDiscovery at Arthur Cox, Ireland (Dublin)
- Ines Rubio, Senior Director of Technology at FTI Consulting, Ireland (Dublin)
- Yelizaveta Kotova, eDiscovery Attorney at Reed Smith, USA (Pittsburgh, PA), Co-Trustee