ARCHER
ATTORNEYS AT LAW

PRACTICAL IMPACT OF GDPR ON U.S. LAW FIRMS

1. Are US law firms subject to the GDPR?

(a) Short answer is yes - if your law firm (even if it employs less than 250 people) offers (**not limited to provides**) services to clients **in** the EU; if your firm collects and/or monitors data of EU citizens (**in whatever less than occasional capacity**); if your firm participates regularly in matters involving EU citizens personal information; if your firm regularly communicates with EU citizens, your firm may be subject to the GDPR. Article 3 (2). https://www.biggerlawfirm.com/u-s-lawyers-should-your-firm-be-gdpr-compliant/

(b) Law firms subject to the GDPR are controllers and probably processors as well in some cases.

(c) Article 4 of the GDPR defines each of these types of data handlers as follows:

- **Processors** are defined as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."

- **Controllers** are defined 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."
- **In general**, a controller decides how personal data is processed, while a processor, as the term suggests, carries out the actual processing of data based on direction from the controller. Controllers are responsible for ensuring that any and all processors they do business with are in compliance with GDPR, although both processors and controllers can be liable if they're responsible for a breach.

(d) US law firm as a "controller" - according to the ICO in the UK:

Advising clients as to legal rights vis-a-vis data subjects. An attorney should be considered a controller when he or she receives personal data about a third party in order to advise the client concerning its rights vis-a-vis the third party data (e.g., a client shares personal data about a former salesman that stole client information).

Client defers to attorney concerning use of data. An attorney should be considered a controller when a client has "little understanding of the process the solicitors will adopt or how they will process the personal data" during the course of providing a representation.

(e) US law firm as a "processor" – litigation.

Attorney acts as a discovery processor in litigation. Law firm has data production facilities and personnel who determine (at the client's direction or acquiescence) how documents with personal information are collected, stored and disseminated in the litigation. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/

(f) Joint or Separate Data Processor? Article 26 of the Reg.

Who is in control of the data? The lawyer takes direction from the client who furnishes the data. The lawyer obtains personal information from third parties and furnishes it to the client. The client and the lawyer work closely on the case including the data obtained and deciding what to do with it. Does the lawyer control the data if the client has input? Is there a joint agreement (retention letter with client specify or elsewhere)?

2. Personal data under Article 4 – what is personal data subject to GDPR?

(a) Data protection is a fundamental right in European Law. Article 8 of The European Charter of Fundamental Rights enshrines the right of every citizen to "the protection of personal data concerning him or her". The European Union Charter of Fundamental Rights,

Article 8, paragraph 1. "Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law". The European Union Charter of Fundamental Rights, Article 8, paragraph 2.

(b) Under the GDPR, "personal data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

(c) According to the European Commission, personal data includes: a name and surname; a telephone number; home address; a personal email address; an identification card number; location data (for example the location data function on a mobile phone); an Internet Protocol (IP) address; a cookie ID; the advertising identifier of your phone; data held by a hospital or doctor, which could be a symbol that uniquely identifies a person.

(d) The law protects personal data regardless of the technology used for processing that data – it's technology neutral and applies to both automated and manual processing, provided the data is organized in accordance with pre-defined criteria (for example alphabetical order). It also doesn't matter how the data is stored – in an IT system, through video surveillance, or on paper; in all cases, personal data is subject to the protection requirements set out in the GDPR. https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

3. Client vs. Third-Party Personal Data (Lawfulness of Processing).

(a) Article 6 1(a), the data subject has given consent – obtain client consent to process their personal information prior to the commencement of the engagement. Include explicit, required consent language in the engagement letter or by separate document? Article 7 part 2 requires clear language which is "clearly distinguishable from the other matters" in the document. Probably not sufficient just to have a check the box on your website.

(b) What if the client withdraws its consent? The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. Article 7, section 3. Ethical implications? Client withdraws consent prior to termination of the engagement.

(c) Rules of Professional Responsibility (3.4(a)) provide that a lawyer has a duty to preserve evidence. American Bar Association, Model Rules. What if the lawyer receives a demand from opposing counsel to hold and preserve all evidence (**a litigation hold letter**) and a simultaneous withdrawal of consent from the client and objection to further processing or a demand for his/her "right to be forgotten?" Art. 17.

(d) Duty to third-parties relative to personal information. Lawyer knows that in the process of discovery he/she will be collecting personal information from or relative to third parties. Does counsel need to obtain consent from witnesses and other parties with relevant evidence or information? Can counsel obtain a court order dispensing with this requirement? Will it be binding outside of the US?

(e) 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. Article 6 1(b). Does this give the lawyer a pass (exception) to consent or withdrawal of same? As to the client, maybe? As to third parties probably not.

(f) Processing is necessary for compliance with a legal obligation to which the controller is subject. Art. 6 1(c). Exception to consent or request to delete? US Court Order, Court Rules or Ethical Rules binding on an EU citizen? Probably best to get language in the Court Order.

(g) 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. Art. 6 1(e). What if the lawyer is handling a pro bono case? What if lawyer or his client is a Trustee or some other type of fiduciary? Does this obviate or override consent?

(h) 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. Art. 6 1(f).

(i) Recital 47 clarifies somewhat the concept of the weighing of interests to determine if consent is required:

> The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. Given that it is for the legislator to provide by law for the legal basis for public authorities to

process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks. The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.https://www.gdpreu.org/the-regulation/key-concepts/legitimate-interest/

The Article 29 Working Party cautions that the balancing test should be documented in such a way that data subjects, data authorities, and the courts can examine. It should encompass a broad range of factors including "any possible (potential or actual) consequences of data processing". This would include, for example, "broader emotional impacts" and the "chilling effect on … freedom of research or free speech, that may result from continuous monitoring/tracking".

(ii) Solutions? Invest heavily in consent or process information which is not personal data subject to protection under the GDPR. https://pagefair.com/blog/2017/gdpr-legitimate-interest/.

(iii) Law firm has no choice but to invest heavily in data protection including obtaining consent and keeping the client and/or third-party continually informed of the use of their personal data. May be true for client information (cannot anonymize client information for the most part) but potentially true for third-party information collected in course of the representation of the client ? **Huge compliance cost in terms of delay, prejudice to client and money**.

(i) **Anonymization v. pseudonymization**. Anonymized data is data which is stripped of any discrete identifiable information of the individual such that the subject cannot be re-identified based on that data even by the anonymizer. Psuedonymization allows the processor to store otherwise identifiable information separately such that it can only be used to identify the subject when put together. Article 4 (5) of the GDPR defines pseudonymization as "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information." By holding the de-identified data separately from the "additional information," the GDPR permits data handlers to use personal data more liberally without fear of infringing the rights of data subjects. This is because the data only becomes identifiable when both elements are held together.

(j) From a law firm's perspective either option above seems over burdensome and very costly as well as inefficient, particularly in litigation. Easier to obtain client or third-party consent or a court order, particularly in cases where significant volumes of personal data are being collected and/or processed by the law firm. Examples: discovery which yields large volumes of personal data; mailing matrices with personal data; creditor or other trust beneficiaries, stock holders. How does the attorney obtain a court order where no case is

pending but he/she is now in possession of large amounts of personal data under the GDPR? Consent is time consuming and costly. Is there another applicable exception?

4. Appointment of a DPO (Data Protection Officer). Art. 37.

(a) Under the GDPR, you **must** appoint a DPO if:

(i) you are a public authority or body (except for courts acting in their judicial capacity);

(ii) your core activities require large scale, regular and systematic monitoring of individuals (for example, online behavior tracking); or

(iii) your core activities consist of large scale processing of special categories of data or data relating to criminal convictions and offenses. GDPR defines "special categories" of data as "information about a person's racial origin, political opinions, religious or similar beliefs, trade union membership, or physical or mental health condition or sexual life." Art. 9, (1). Consent and other exceptions may apply including to establish a claim or legal defense. Art. 9 (2)(a)(f).

(iv) Law firm may fit into (iii) above? Depends on the firm's business and collection and/or processing of personal data. Most firms will not require appointment of a DPO unless they are involved in certain types of representations on a large scale, frequent basis. Probably limited to larger firms or firms that specialize in certain matters under (iii) above. If your firm has a presence in the EU, it is potentially subject to the GDPR no matter what.

(b) Law Firm may nevertheless elect to voluntarily appoint a DPO. Art 37 (4).

5. Appointment of a Representative in the Union. Art. 27.

(a) Where Article 3 (2) applies, you must appoint a representative in the Union unless:

(i) processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or

(ii) a public authority or body.

(b) Law firm compliance? Probably not many firms fit in this category similar to 4 above. Larger firms may already have an "establishment" with a representative in the Union to designate. Medium to smaller firms will argue occasional processing exception above.

Occasional is not defined under the GDPR. Query: What if your law firm frequently enters into engagements with Union clients or case involving Union third-parties and, in the process is in control of or processing personal information of those citizens of the Union? Do you need a representative in the EU?

6. Data Processing Records.

(a) Article 30 sets out a lengthy requirement for Controllers and Processors to document their processing activities of personal data. Records of such activities may be electronic and must be made available to the Supervisory Authority upon request.

(b) Exception applies to an organization employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9 (1) or personal data relating to criminal convictions and offences referred to in Article 10. Art. 30, (5).

(c) Again, a smaller law firm may utilize the exception in (b) depending upon its size, on type of data being collected or processed and the frequency of its collection or processing.

7. Processing of the Data. Article 5.

(a) Personal Data must be:

(i) processed lawfully, fairly and in a transparent manner in relation to the data subject. **Transparency implies that any information and communication concerning the processing of personal data must be easily accessible and easy to understand. Also, clear and plain language needs to be used in this regard. More specifically, this principle ensures the data subject receives information on the identity of controllers and purposes of the processing of personal data.** Is this feasible for the US attorney, for any attorney dealing with volumes of third-party information in heated, costly litigation, from or related to EU data subjects?

(ii) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

(iii) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. **Who is the arbiter of what is adequate? When it comes to US discovery, the limits are wide and the exploration often deep. Not so in the EU!**

(iv) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. **Probably easier for the controller or**

processor when dealing with client information but nearly impossible with certain third-party information.

(v) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.

Ethical rules require attorneys in the US to retain client property (including files and client information until the engagement is complete and often firms retain such information for years following the engagement in case matters arise where such information is needed.

In a 1977 informal opinion, the ABA Committee on Ethics and Professional Responsibility specifically refused to mandate a definitive time period during which a lawyer must preserve all files and beyond which s/he is free to destroy all files, advising instead that an attorney must use "good common sense." While noting that "a lawyer does not have a general duty to preserve all of his files permanently," the Committee cautioned against the destruction of original documents belonging to the client, the discarding of information that may be useful in the assertion or defense of the client's position, or the destruction of information that the client may need, has not previously been given to the client, and is not otherwise readily available to the client, and which the client may reasonably expect will be preserved by the lawyer. (ABA Com. on Ethics & Prof. Resp., informal opn. No. 1384 (1977).

(vi) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

Attorney must take reasonable steps to protect and secure the client's information (Cal. State Bar Formal Opn. No. 2012-184; Cal. State Bar Formal Opn. No. 2010-179.) • Must ensure confidentiality (e.g., choose data service providers with care, and use firewalls, secure user names & passwords, encryption, anti-virus software etc.) • Must ensure digital backups exists (extra hard drive, storage in the "cloud", off-site server, etc.) • Must ensure electronic files are maintained in readily-accessible format (i.e., no more floppy disks!) • Must ensure your designated successor counsel knows how to access the information if necessary (identity of passwords, location of hard drives) • Try to save documents in non-modifiable format (e.g., .PDF rather than Word .DOC version).

(b) As a practical matter, as to clients, most sophisticated law firm already have fairly stringent IT processes and safeguards in place to collect, store, manage and ultimately

delete client data. The task, however, with third-party personal data the law firm acquire is infinitely more complicated.

(c) **Example**, during the course of representing a US subsidiary of an EU parent (insert the type of matter here: litigation, insolvency proceedings, corporate M&A, IP rights, transfer pricing), the law firm collects and/or processes volumes of data relative to EU data subjects. Does the law firm need a separate protocol for processing that information under the GDPR? Answer is, probably yes. It would not be sufficient to simply store it somewhere electronically and/or in hard copy and eventually delete it or throw it away years later. Costs of compliance are high here.

8. Rights of the Data Subject (Articles 12-23).

(a) Article 12, Right of Access of Data Subject.

(b) The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(i) the purposes of the processing;

(ii) the categories of personal data concerned;

(iii) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations;

(iv) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(v) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(vi) the right to lodge a complaint with a supervisory authority;

(vii) where the personal data are not collected from the data subject, any available information as to their source;

(viii) the existence of automated decision-making, including profiling, referred to in Article 22 (1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(c) **What is the import of all this for law firms? You had better get consent from the data subject pursuant to proper notice and election or have a court order if possible exempting such compliance or fit one or more of the other "exceptions" to compliance without consent in Article 6.**

(d) EU client consent is a given-must get it. Third-Party consents may be difficult or unobtainable. Do you fit another exception? What if the third-party demands erasure or objects to further use of information during the engagement? If you obtain information about third party data subjects during the course of representation do you have to give them notice under Article 12 in compliance therewith? Probably, yes. If you don't and a complaint is filed in the EU with the authority **or against you**, then what? Will third-party's and defendants in the EU use the GDPR as a litigation tactic to impede the flow of evidence or slow down the matter? What if your firm receives a complaint for non-compliance in the middle of the litigation? What if notifying the third-party data subject might cause damage to your case or recovery? Impact to the client could be devastating.

9. Notice to Data Subject Required where Data is Obtained from the Subject. Article 13.

(a) Must give the data subject, upon receipt of data, notice of:

(i) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(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) where the processing is based on point (f) of Article 6 (1), the legitimate interests pursued by the controller or by a third party;

(v) the recipients or categories of recipients of the personal data, if any; **AND**,

(vi) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(vii) 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;

(viii) where the processing is based on point (a) of Article 6 (1) or point (a) of Article 9 (2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(ix) the right to lodge a complaint with a supervisory authority;

(x) 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 obliged to provide the personal data and of the possible consequences of failure to provide such data.

(b) See, 8(d) above.

10. Article 14, Notice to Data Subject, Data from other Sources.

(a) Must give data subject notice of controller.

(b) Additional notice requirements substantially similar to Article 13.

11. Data subject has a right of access under Article 15 to data and related information concerning use and storage, erasure etc.

12. Articles 16-21.

(a) Largely consist of data subjects rights to receive the personal information, to clarification of personal information, to erasure or deletion of data, to restrictions on use and the right to object to processing or retention of data.

(b) Calls into question whether the cost of compliance is worth the business?

(c) Unintended consequences of the GDPR.

https://www.csoonline.com/article/3260738/regulation/what-unintended-consequences-the-general-data-protection-regulation-could-have.html

https://www.pymnts.com/news/regulation/2018/eu-gdpr-big-tech-backlash-consumer-data-privacy-cost-of-noncompliance-consequences/

https://martechtoday.com/after-gdpr-here-come-the-unintended-consequences-216125

13. Can law firms do the same-eliminate or reduce exposure? Probably.

(a) Add privacy notices to engagement letters.

(b) Limit business in EU to occasional.

(c) Establish protocols with professionals internally to safeguard against becoming subject to GDPR compliance; i.e., IT, intake, attorneys and staff.

(d) Establish and document exceptions to compliance. Obtain court orders; sophisticated party waivers (effective?); rely on contrary local law (legislation, case law).

(e) Rely on Article 23. Restrictions on applicability of Article 5, Articles 34, 12-22. Local State law in EU may restrict applicability or modify it. Similar law in US? Argue that EU State law should apply given where the subject resides. Legal independence exception (preserve integrity of the US legal system)?

(f) Don't do business with EU data subjects. Revenue may not justify compliance costs or fines. http://fortune.com/2018/05/25/gdpr-compliance-lawsuits/

14. Security Measures-Article 32. Imposes a high cost of compliance from a technology perspective on small to medium sized firms.

15. Data Breach-Articles 33-34.

(a) In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, **unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.** Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

(b) When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

(c) The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

(d) The data breach communication to the data subject shall not be required if any of the following conditions are met:

(i) the controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption;

(ii) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialize;

(iii) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

(iv) If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

16. Security and Impact Assessment. Articles 32 and 35.

(a) The assessment shall contain at least:

(i) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(ii) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(iii) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

(iv) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

(b) Cost of Compliance.

(i) https://www.prnewswire.com/news-releases/us-companies-projected-to-spend-417-bn-on-compliance-with-the-eus-gdpr-legislation-682812501.html

(ii) https://www.pacificdataintegrators.com/insights/Yes-GDPR-Compliance-is-Worth-the-Cost

(iii) Will your firm obtain certification that it is compliant? Article 42. Huge measure of client confidence if your website has a certification of GDPR compliance in it.

17. Remedies, Liabilities and Penalties.

(a) Articles 77-79.

(i) Right to lodge a complaint with the supervisory authority.

(ii) Right to exercise judicial remedies against the supervisory authority in court.

(iii) Right to exercise judicial remedies against the controller or processor in court.

(b) Representation of Data Subjects. Article 80.

Data subject can seek out a non-profit or similar organization to request filing of an action on his/her/its behalf!

(c) Right to Compensation and Liability.

(i) Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

(ii) Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

(iii) A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.

(iv) Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.

(v) Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.

(vi) Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79 (2).

(vii) Enforcement in the US? https://politics.stackexchange.com/questions/30509/how-are-gdpr-fines-actually-enforced-for-us-companies-with-no-physical-presence

(d) US Litigation and Legislation so far.

(i) Not much litigation yet over GDPR in the US. Much of it has been over lowering of stock prices given the target companies lack of preparedness and significant outlays which have impacted earnings. https://www.dandodiary.com/2018/08/articles/securities-litigation/investors-filed-gdpr-related-securities-suit-nielsen-holdings/

(ii) March, 2018, EU Parliament appears in US Supreme Court. Clearly there are conflicts in US law with the GDPR. https://www.fisherphillips.com/Employment-Privacy-Blog/gdpr-compliance-collides-with-u-s-law

(iii) States in US are starting to enact privacy laws similar that of the EU. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

(iv) Call for US Federal Privacy Regulation. November, 2018 Federal Bill Introduced. To amend the Federal Trade Commission Act to establish requirements and responsibilities for entities that use, store, or share personal information, to protect personal information, and for other purposes. https://www.wyden.senate.gov/imo/media/doc/Wyden%20Privacy%20Bill%20Discussion%20Draft%20Nov%201.pdf

215771292v3