Perspectives on the
General Data Protection Regulation
Of the European Union

Prepared Remarks of

Peter H. Chase
Senior Fellow
German Marshall Fund of the United States

To the Hearing on

"Privacy Rights and Data Collection in a Digital Economy"

Before the

Committee on Banking, Housing and Urban Affairs
Of the United States Senate

May 7, 2019

Chairman Crapo, Senator Brown, Members of the Committee:

Good morning and thank you for providing me the opportunity to offer some perspectives on the European Union's General Data Protection Regulation (GDPR), as the Committee considers whether and how the United States should adopt a comprehensive data protection law.

My name is Peter Chase; I am a Senior Fellow at the German Marshall Fund of the United States, a 501(c)(3) nonpartisan and not-for-profit organization based in Washington, D.C. GMF was established in 1972 by a gift from the German government to recognize the 25th anniversary of the Marshall Plan to rebuild Europe after World War II, and is dedicated to promoting transatlantic cooperation in the spirit of that Plan. The views I express are mine alone. I am not speaking for the German Marshall Fund of the United States, which does not take institutional positions on policy issues.

My perspectives on the GDPR are based on nearly a quarter-century of work on economic relations between the United States and the European Union (EU), first as part of my 30-year career as a U.S. Foreign Service Officer,[1] then when representing the US Chamber of Commerce in Europe from 2010 to 2016, and now with GMF. My primary interest in the EU's data protection regime has been on the provisions concerning transfers of personal information to

[1] I was assigned to the U.S. Mission to the European Union in 1992, when the EU was considering the GDPR's predecessor, the Data Protection Directive. I continued to work on the issue when I served in the U.S. Embassy to London and as the Chief of Staff to the Under Secretary for Economic Affairs as the U.S. and EU were negotiating the Safe Harbor Agreement, and ran again into data protection issues again when assigned to the U.S. Mission to the European Union in 2007-2010.

third countries like the United States, in the law enforcement and national security context as well as for the private sector, although I of course have been concerned with the other aspects of that regime as well. In this context, I will try to provide an objective description and assessment of the GDPR. I will note my personal views and opinions when offering those.

My comments will cover three aspects of the GDPR:
-- its antecedents and political context;
-- its provisions; and
-- its implementation.

The European Union

But first, a word on the European Union, as the GDPR in many respects reflects the evolution and structure of the EU. The European Union stems from a series of international treaties concluded in 1957 initially among six countries, a number that progressively increased to 28 today. The underlying ethos of the treaties is that closer integration can prevent Europe from being engulfed again by the conflagration of war. In acceding to the EU, countries take the sovereign decision to promote that integration by jointly making laws that apply in each of their territories.

In this structure, all law and regulation must first be proposed by the **European Commission**, which is intentionally independent of any member state, but these proposals only gain legal effect if adopted by the **EU Council**, representing the sitting governments of the member states, and the **European Parliament**, directly elected representatives of the population in each member state. (The Council is often likened to the U.S. Senate, and the European Parliament to the House of Representatives; indeed a process akin to our conference committees is needed for the two to agree on a single final text.) EU laws generally take two forms – **Directives** that member states implement through national law, and **Regulations** that have direct effect. The European Court of Justice (ECJ), like our Supreme Court, ensures that laws, both at the EU and national levels, are consistent with the underlying EU Treaties.

GDPR's Antecedents and Political Context

The immediate predecessor to the General Data Protection Regulation was the Data Protection Directive, adopted in 1995 on the basis of a proposal originally submitted by the Commission in 1990. At the time of the proposal, establishing a Single Market among the then 12 members[2] of the European Economic Community (as it was then known) was the top priority. The Commission argued that seven member states[3] had adopted national data protection laws, and that this "*diversity of national approaches and the lack of a system of protection at the Community level are an obstacle to the completion of the Single Market …. (such that) the cross-border flow of data might be impeded just when it is becoming essential to the activities of*

[2] Denmark, Ireland and the United Kingdom having joined Belgium, France, Germany, Italy, Luxembourg and the Netherlands in 1973, while Greece joined in 1981 and Spain and Portugal in 1986.
[3] Denmark, France, Germany, Ireland, Luxembourg, the Netherlands, the United Kingdom.

business enterprises and research communities ….”[4] At the time the European Economic Community did not cover fundamental rights of individuals, but the Commission asserted the importance of these as expressed in the European Convention on Human Rights under the Council of Europe (a separate international organization). Indeed, it harkens back to the 1981 *Council of Europe Convention 108 for the Protection of Individuals with Regard to the Automated Processing of Personal Data* (pursuant to the ECHR protection of privacy) as well as the *1980 OECD Guidelines on the Protection of Privacy and the Cross-Border Flow of Personal Data* as both the ethical and intellectual foundations for the high level of protections of personal data that the Proposal recommends. (It also calls for the Community itself as well as the five member states that had not acceded to Convention 108 to do so.)

While many of the specific provisions of the 1990 Commission proposal for the Data Protection Directive are reflected in the version as eventually adopted in 1995, the political context changed significantly in the meantime, including through the 1993 entry into force of the Maastricht Treaty. This created the construct of the European Union as a “roof” over the European Community, complemented by two new “pillars” of *intergovernmental* cooperation among the member states in the areas of law enforcement and foreign policy.

The Maastricht Treaty also strengthened the role of the European Parliament in law making, which arguably increased the Directive’s emphasis on protecting personal data as a fundamental right. This increased emphasis, however, also reflects the political significance of the fall of the Berlin Wall, the collapse of the authoritarian regimes of the Warsaw Pact countries and the reunification of Germany (which brought additional members to the European Parliament), as well as the expansion of the EU to include Austria, Finland and Sweden in 1994.

It is often said that the importance of data protection as a fundamental right reflects Europeans’ sensitivity about government spying, especially under the Stasi and the Communist governments in Central Europe. This is true, in part. But the 1995 Data Protection Directive applies primarily to commercial processing of data, and to that of the governments in the “normal” course of their business; law enforcement and intelligence functions are explicitly outside the scope. And indeed, my recollection of the debate during that time was that much of the concern was more about direct mail advertising and spam, rather than civil liberties.

The political context changed dramatically between the 1995 adoption of the Data Protection Directive and the adoption, in 2016, of the General Data Protection Regulation. I will highlight some of the key differences in the provisions between the two below, but here the critical contextual changes include:

- the conclusion of the Charter of Fundamental Rights and Freedoms of the European Union in 2000; although not at that time a legal text of the European Community, the Charter brought a fundamental right to privacy and to data protection into the general legal regime of the Community as all the EU institutions pledged to respect it;

[4] Commission of the European Communities, Communication on the Protection of Individuals in Relation to the Processing of Personal Data in the Community and Information Security, COM(90) 314, 13 September 1990, page 4.

- the accession into the EU of virtually all of the former Warsaw Pact countries in 2004[5] and 2007;[6]
- the entry into force of the Lisbon Treaty in November 2009, which inter alia:
    - gave the European Union legal personality;
    - integrated the law enforcement and foreign policy pillars into the EU structure (as opposed to having the Commission support inter-governmental cooperation); and
    - formally incorporated the EU Charter of Fundamental Rights into the EU Treaty.[7]

Thus, while the 2012 Commission proposal for a General Data Protection Regulation to update the 1995 Data Protection Directive talks about both the huge evolution in technology in the intervening 17 years as well as the frictions created in the Single Market by the many national laws that were required to implement the Directive, that proposal placed a much greater emphasis than the 1990 proposal on the importance of individual's fundamental right to privacy and to control the use of personally identifiable information.

This then snowballed with the Snowden revelations in 2013 of US government access to data held by major American IT firms, which among other things led the Commission, the much enlarged and varied European Parliament, and all the bodies entrusted with interpreting and enforcing the Data Protection Directive to significantly strengthen all the protections that the Regulation provided.

The General Data Protection Regulation

Whereas the 1995 Data Protection Directive has 34 Articles and is 19 pages long, the General Data Protection Regulation (hereafter GPDR) has 99 Articles and is 88 pages long (with very small print!).

Direct Effect, "Pre-emption"

The most important legal difference between the two is that GDPR is a Regulation, having direct legal effect in the territories of all 28 EU member states as of May 25, 2018. In providing this uniform direct effect, GDPR eliminates obstructions to data flows (potentially) caused by divergences in national law, thus "ensuring" the primary objective of allowing the free flow of personal data within the European Union. In that sense it "pre-empts" all existing national data protection laws, although it provides some instances where the member states either may or must adopt certain accompanying legal measures (e.g., to strengthen the powers of the national Data Protection authorities).

Expansive Scope

Like the Data Protection Directive, the GDPR is an **omnibus bill** covering virtually all "**processing**" by both government and non-government entities of **personally identifiable**

[5] The Czech Republic, Estonia, Hungary, Latvia, Lithuania, Poland, Slovakia, Slovenia.
[6] Bulgaria and Romania.
[7] Although, in so doing, explicitly not expanding the European Union's powers beyond those actually in the EU Treaties.

information (PII), where PII is expansively defined as "any information related to an identified *or identifiable* natural person" (including online identifiers like an IP address), and where "processing" means "any operation performed on personal data, *whether or not by automated means*." Not covered is processing by governments that does not fall within the scope of the EU Treaties or is related to national security or law enforcement, as well as that done by individuals for purely personal reasons.

Processing of any PII of anyone in the world done in the territory of the EU is of course covered, but so too is that done by anyone *outside* the EU if that processing:

- includes information of residents in the EU and is done on behalf someone in the EU (who is then responsible for how it is processed); or
- is done either to offer goods and/or services to someone in the EU (that is, for a commercial reason) or to "monitor behavior" of a person where that behavior takes place in the EU.

With this hugely expansive scope, GDPR then lays out:

- Principles related to the processing of personal information;
- Rights of individuals whose data is processed;
- Obligations on "controllers" of PII doing the processing (as well as "processors" who process data on behalf of the controllers);
- Restrictions on the transfer of PII outside the European Union; and
- A series of administrative and enforcement measures.

The most important aspects of each of these parts are described briefly below, with a bit of additional detail on three of the most critical (consent and the other legal bases for processing, profiling and automated decision-making) discussed in the third section on implementation.

Data Processing Principles

GDPR specifies that anyone that has and processes personal data is accountable for ensuring that such data is:

- Processed in a legal, fair and transparent fashion (lawfulness);
- Collected and used only for specified, explicit and legitimate purposes (purpose limitation);
- Limited only to what is necessary for the specific purpose of processing (data minimization);
- Accurate, with inaccurate data rectified and erased (data accuracy);
- Retained only as long as needed (data retention); and
- Protected (integrity and confidentiality).

There are six legal grounds for processing personal information under the "lawfulness" principle, determined by whether the controller:

-- has the consent of the individual ("freely given, specific, informed and unambiguous"); OR
-- needs to do it to perform a contract with that individual; OR
-- must comply with a legal obligation spelled out in law; OR
-- believes so doing is in the "vital interests" of the individual or another person; OR

-- will do so for a public purpose, again spelled out in law; OR
-- can demonstrate that so doing is in the "legitimate interests" of the controller or a third party, as long as such interests are not over-ridden by those of the individual.

The processing of "special categories" of personal data (racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic and biometric information, health or sexual orientation) is **prohibited**, *unless:*[8]

- The individual provides explicit consent (stronger than informed consent);
- the information is already "manifestly made public" by the individual;
- the processing is necessary related to employment or social security;
- the processing is done by a foundation, political, trade union or other non-profit body for the purposes of that body; or
- there is a substantial public, scientific, medical or research reason to do so.

Rights of the Individual

GDPR's Third Chapter empowers individuals to ensure they:

- Understand what PII is being collected, by whom, for what specific purpose and on what legal grounds, who will have access to it (whether a processor, or a third party, including if overseas), and how long it will be retained; *this applies whether the data is collected directly from the individual or not;*

- Can access their PII held by a controller;

- Can rectify the data so held, and demand its restricted use or erasure ("right to be forgotten") when it is no longer needed, the individual has withdrawn consent, the processing is done without a legitimate basis, or the individual objects to the processing, although the exercise of these rights cannot interfere with others' right to freedom of expression and information, compliance with a legal obligation, public health needs, or legal claims;

- Can receive and transfer this data to another controller ("portability");

- Can object to any processing based on the "legitimate needs" grounds noted above, and particularly to processing for direct marketing, and profiling related to that; and

- Are not subject to a "decision based solely on automated processing (including profiling) … which produces legal effects or similarly significantly affects him or her."

EU or member states can restrict these rights for a number of reasons (national security, law enforcement, etc.) but the laws must clearly spell out why such restriction is necessary.

[8] The ten exceptions in Article 9(2) from processing sensitive data are more detailed than presented here.

Obligations on the Controller/Processor

Any "controller" that has personally identified information (or a "processor" working on that data on behalf of the controller) is legally responsible for implementing "appropriate technical and organizational measures" to ensure that the principles and individual rights spelled out above can be effected. In particular, they must:

-- ensure they have a specific legal grounds for any processing;
-- provide users clear and easily understandable information about the data they will collect, how it will be used and the specific legal grounds on which it will be processed, who will have access to it, etc.;
-- grant access to and copies of any PII they hold on request, and comply with withdrawals of consent, requests for amendment, and restrictions on or objections to processing (with the exceptions noted above);
-- use technical means such as "pseudonymization," encryption and data protection by design/default to ensure data minimization;
-- conduct "data protection impact assessments" prior to any new processing that may involve high risks to individuals' rights (including profiling and automated decision-making), in consultation with the appropriate national data supervisor;
-- keep records related to their data processing;
-- provide appropriate security/protection for the data, notifying supervisory authorities (and if appropriate, individuals) of data breaches; and
-- appoint a data protection officer, if they are a public authority, regularly process large amounts of PII, or deal in large amounts of personal data. Otherwise, firms should be able to access a data protection officer through, for instance, their industrial association.

Adherence to Codes of Conduct or other certification schemes can be used to help demonstrate compliance.

Controllers or processors not established in the Union must have a representative in the EU to ensure they can be held legally accountable, although this does not apply if they are a public authority or their processing is "occasional" and doesn't include large amounts of sensitive data.

Third Country Transfers

Transfers of personal data out of the EU should in principle "take place *only* if" ("prohibited" is the word used in Recital 107) the "level of protection of natural persons guaranteed by this Regulation is not undermined." In particular, transfers can take place if:

-- the Commission deems a country provides an "adequate" level of protection (which it has done for six countries outside Europe, most recently Japan, as well as for U.S. firms that adhere to the U.S.-EU "Privacy Shield" arrangement);
-- appropriate safeguards exist in the form of contract clauses, binding corporate rules, adherence to Codes of Conduct or certification schemes;
-- the individual has given *explicit* consent to the transfer;
-- the transfer is necessary for performance of a contract or in the public interest, etc.

Otherwise, transfers may only take place where it is not repetitive, does not involve many individuals, is in the "legitimate interest" of the controller (to the extent that the individual's interests don't override those), AND where the controller has assessed the risks associated with the transfer, established appropriate safeguards and informed individuals of the risks involved.

Implementation and Enforcement

Chapters 6, 7 and 8 of the GDPR go to its administration and enforcement. As noted above, a primary objective of the GDPR is to ensure the free flow of data within the EU and the consistent application of the law through a Regulation that has direct effect in the territories of each member state. To that end, one of the novel aspects of the Regulation is the notion of a "lead" supervisory authority that oversees and regulates the activities of companies operating in a number of member states. The GDPR accordingly strengthens the roles, responsibilities, powers (including investigatory and "corrective") and independence of the member state data protection authorities (many of which have been upgraded to Commissions). It further establishes a European Data Protection Board (EDPB) in which they are all represented and which is designed to facilitate cooperation among them, adjudicate differences between them, and issue guidance interpreting the GDPR which they will apply to the controllers and processors in their territory.

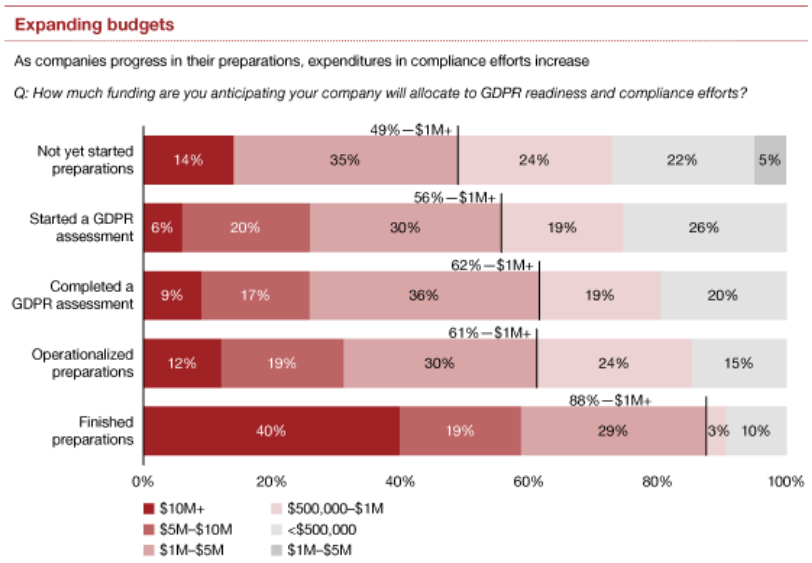
These national data protection supervisors have the authority to issue warnings and reprimands, order compliance with an individual's requests, impose temporary or definitive bans on processing, order restrictions or erasure of data, order suspension of data flows and impose administrative fines, which can be up to €20 million or 4 percent of total worldwide annual turnover (whichever is larger) of a "controller." Decisions of the data protection authorities are subject to judicial review.

GDPR Implementation

The GDPR has been in effect for almost a year, with varying claims about its impact, stringency, efficacy, workability and enforcement.

According to a number of reports, companies – including American firms – have spent literally billions of dollars over the past two years to bring themselves into compliance.[9] Another often-quoted 2018 survey by PwC[10] notes, inter alia, that the more advanced a firm is in its compliance efforts, the greater (and more certain) the budget for compliance is, with over 40% of compliant U.S. companies saying they spent over $10 million each:

[9] Oliver Smith, The GDPR Racket: Who's Making Money from this $9 billion Business Shakedown, Forbes, May 2, 2018.
[10] Pulse Survey: GDPR Compliance Budget Top $10 million for 40% of Surveyed Companies, PwC



And the International Association of Privacy Professionals, perhaps gleefully, once estimated that some 75,000 Data Protection Officers would be needed worldwide to ensure compliance.[11]

Most of this "investment" of course stems from firms' concern about the potentially enormous cost of *not* complying – if the maximum fine of 4% of global sales is applied. Especially in large U.S. and European companies, where lawyers abound and compliance departments have serious clout, not complying with the strictest interpretation of the law as written is not an option. That said, the largest enforcement action to date, at least in terms of penalties, was a €50 million fine imposed on Google by the French data protection authority in January 2019 largely for lack of transparency related to the use of information from its Android system on phones in France. But a small Austrian business was fined in October for the overly broad use of its security cameras, a German social media firm paid €20,000 for poor practices related to a data breach, and a data processor in Poland was fined €220,000 for data scraping and direct mailing about which consumers complained.[12]

And in fact, thus far, most national data protection authorities are focusing on helping and advising local firms on implementing the GDPR and adopting "good" data processing practices. As such, most of the thousands of enforcement "actions" that have occurred over the last ten months have involved amicable resolutions, warnings and advisory steps.[13]

---

[11] Rita Heimes and Sam Pfeifle, Study: GDPR's Global Reach to Require at Least 75,000 DPOs Worldwide, IAPP, November 9, 2016.

[12] Steven Pinson, The Need for United States and Canadian Businesses to have a GDPR Compliance Initiative in Place is Paramount, Mondaq, February 1, 2019 (accessed April 30, 2019).

[13] See, for instance, Data Protection Commission of Ireland, Annual Report (May 25, 2019-December 31, 2019), 28 February 2019, which notes that it had received 2,864 formally-recognized "complaints" since GDPR entered into effect (and an additional 612 prior to May 25), of which 868 had been concluded (usually amicably, but leading to 32 formal decisions, 13 in favor of the complainant), 510 had proceeded to complaint-handling and 550 were being actively assessed; of the complaints, 136 were by other EU member state data protection authorities to the Irish DPA as the lead supervisory authority for multinational firms based in Ireland.

In this sense, some of the warnings about the negative effects of the GDPR have been over-blown. GDPR itself is very prescriptive, and the right of every individual to ask a company for information about the data it holds on him or her, and to file a complaint, undoubtedly implies a lot of additional work (and cost). But very few data processing activities – including profiling for direct-marketing/advertising purposes -- are actually prohibited, although they can no longer be undertaken with impunity. And while Data Protection Authorities must respond to all complaints, they have discretion about how to handle them. Further, while GDPR may not be directed solely toward addressing identified *tangible* "harms," it is risk-based and emphasizes situations that involve processing of large amounts of personal data (especially if that processing includes sensitive information) from large numbers of individuals.[14] Bigger companies, especially in the IT sector (but also many others, including auto and energy companies), are accordingly much more likely to be watched. Knowing this, many such companies have spent the last two years carefully scrutinizing their own data collection, use and retention policies, a "data hygiene" process that some now welcome (albeit usually in hind-sight).

GDPR Guidance

Indeed, in some respects the most important implementation steps that have happened are the guidance documents issued by the newly-constituted European Data Protection Board, the successor of the so-called Working Party 29 (WP-29) that was established under Article 29 of the previous Data Protection Directive. Some of these guidance documents are interpretations by the WP-29 of the GDPR following its adoption but prior to its entry into force in May 2018, which are largely on issues where the GDPR and its predecessor are similar. Since, the EDPB has either adopted many of these WP-29 documents (giving them more force than they had under the old law) or issued its own documents for public comment and then as final "rulings."

These guidance documents go to some of the most controversial provisions of the GDPR, including the notions of consent and contracts as legal bases for processing, and about profiling, automated decision-making and "artificial intelligence," all discussed further below.

Consent: The guidance on consent[15] helps clarify the issue of lawful processing in part as it underscores (repeatedly) that informed and unambiguous consent is *only one* of the bases for processing, and indeed that it often is not the best one. Among other things, it stresses that "inviting people to accept a data processing operation should be subject to rigorous requirements, since … *the controller wishes to engage in a processing operation that would not be legal without the data subject's consent*." It further specifies that controllers cannot "bundle" consent permissions; individuals must consent to each specific processing use of their data at a "granular" level, and must have the right to withdraw their consent from each specific use without that affecting their enjoyment of the other aspects of the offering, especially when the collection or processing of the PII is not strictly necessary for the performance of the contract (although it might be useful for advertising purposes). (For instance, a bank cannot ask for PII to

[14] This is most obvious in the requirements behind the need for a "Data Protection Impact Assessment;" see, e.g., Irish Data Protection Authority, List of Types of Data Processing Operations Which Require a Data Protection Impact Assessment, 15 November 2018.

[15] Article 29 Working Party, Guidelines on Consent under Regulation 2016/679, adopted on November 28, 2017, as last Revised and Adopted on 10 April 2018.

be used for direct marketing purposes in connection with the opening of a bank account.) Given the "imbalance of power," governments/public authorities and employers should never rely on consent, as it cannot be freely given in these contexts. Further, getting consent must be matched by an equally easy-to-do withdrawal of that consent, subjecting controllers to possible requirements to delete PII they may have.

Contracts: But while this WP-29/EPDB interpretation of the limitations on personal consent may "nudge" controllers to other legal bases for processing, those too are strictly interpreted. A draft Guidance document[16] the EDPB has published for three months of public comment on the use of a contract as a legal basis for processing, for instance, notes that while a contract is essential for the conduct of most business relations (including for the conduct of information society services funded through advertising), the principles of purpose limitation and data minimization apply. The EDPB notes, for instance, that where processing is not *in fact objectively necessary* for the provision of the service, other processing (for instance, for direct marketing purposes) can take place only if it relies on another appropriate legal basis (about which the user must be informed). As the Guidance document explains through example:

> *Example 1*
> *A data subject buys items from an on-line retailer. The data subject wants to pay by credit card and for the products to be delivered at home. In order to fulfil the contract, the retailer must process the data subject's credit card information and billing address for payment purposes and the data subject's home address for delivery. Thus, Article 6(1)(b)* [processing under a contract] *is applicable as a legal basis for these processing activities. However, if the customer has opted for shipment to a pick-up point, the processing of the data subject's home address is no longer necessary for the performance of the purchase contract and thus a different legal basis than Article 6(1)(b) is required.*
>
> *Example 2*
> *The same on-line retailer wishes to build profiles of the user's tastes and lifestyle choices based on their visits to the website. Completion of the purchase contract is not dependent upon building such profiles. Even if profiling is specifically mentioned in the contract, this fact alone does not make it 'necessary' for the performance of the contract. If the on-line retailer wants to carry out such profiling, it needs to rely on a different legal basis.*

Automated Decision-Making/Profiling: This sort of very specific, legalistic and protective interpretation of the GDPR ("Data subjects can agree to processing their personal data, but may not trade away their fundamental rights"[17]) is reflected as well in the EDPB's Guidance document on automated decision-making and profiling,[18] which says that:

> "… profiling and automated decision making can pose significant risks for individuals' rights and freedoms which require appropriate safeguards. These processes can be

[16] European Data Protection Board, Guidelines 2/2019, on the processing of personal data of Article 6(1)(b) GDPR in the context of the provision of online services to data Subjects, version for public consultation, April 9, 2019.
[17] Ibid, page 13
[18] European Data Protection Board, Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679, Adopted on 3 October 2017 as last revised and adopted on 6 February 2018.

> opaque. Individuals may not know that they are being profiled or understand what is involved. Profiling can perpetrate existing stereotypes and social segregation. It can also lock a person into a specific category and restrict them to their suggested preferences…. In some cases, profiling can lead to inaccurate predictions. In other cases it can lead to denial of services and goods and unjustifiable discrimination."

The document distinguishes between profiling and automated decision making, although it notes that the former is often a component of the latter. It is also careful to indicate that profiling often comes from the melding of personally identifiable information both provided by the individual *as well as obtained from other sources* to make inferences about likely future behavior, noting how the obligations of transparency and purpose limitation, including on further processing, figure into this. While it does not prohibit either of these processes per se, it holds them to a very high standard, and repeatedly notes the individual's right to object in particular to their use for direct marketing purposes: "It also suggests it would be difficult for controllers to justify using legitimate interests as a lawful basis for intrusive profiling and tracking practices for marketing or advertising purposes, for example those that involve tracking individuals across multiple websites, locations, devices, services or data-brokering."[19]

Artificial Intelligence: The GDPR provisions on automated decision-making and profiling are those most frequently related to "artificial intelligence" (AI, which is not explicitly addressed in the GDPR), as the term "AI" today is frequently used to refer to big data analytics, which often will involve personal information.[20] But European officials argue that these concepts should not be conflated: big data analytics, even that involving PII, is not the same as automated decision-making (defined as a decision about an individual produced "*solely* by automated means"). A controller wanting to engage in big data analytics involving (large amounts of) PII could do so, but only after conducting a Data Protection Impact Assessment to ensure that s/he has an appropriate legal basis to do so and that the rights and freedoms of individuals are not infringed. But where such processing leads to a decision with a significant impact on an individual, the individual has the right to ask for review of that decision by a human.

Conclusion

The EU's General Data Protection Regulation stems from both a need for the European Union to prevent member states from having different regulations that obstruct integration (and cross-border trade in services) by having different data protection norms, as well as a deep belief in the fundamental right to privacy as exercised through an individual's control over the use of data personally identified with him or her.

Europeans argue that a single universal approach to data protection is more effective than a sectoral one, that may only cover certain types of institutions rather than the underlying data that is to be protected, and that organizations outside the sector can abuse.

---

[19] Ibid, page 15.

[20] See, for instance, the excellent discussion of the potential chilling effects of European use of AI in Nick Wallace and Daniel Castro, The Impact of the EU's New Data Protection Regulation on AI, Information Technology and Innovation Foundation (itif), March 27, 2018.

However, in adopting a prescriptive approach to data protection, the EU often assumes, rather than documents, societal harms that its legislation is meant to address. To some extent, EU officials appear to understand that GDPR may be overly restrictive, especially when it comes to the potential societal benefits of big data analytics to masses of personal data; they appear in conversations to be trying to offset this by expanding in some ways the "legitimate interests" of the controller to allow for this.

This, as well as the GDPR provisions on direct marketing, suggest that to some extent the "real" issue the GDPR (as with the Data Protection Directive) is meant to address is the monetization of personal data, where monetization is now meant broadly to include not just advertising, but also benefits from politically-directed micro-targeting of messages.

The GDPR principles, rights and obligations may provide useful guidance for U.S. law-makers as they consider whether the U.S. should adopt analogous legislation. But the specificities of the EU evolution and context should be borne in mind, as should the difficulties the EU addresses as it implements the Regulation. This is one of those instances where the United States, while not having the first mover advantage, may also benefit from moving second.