Centre for Information Policy Leadership
Hunton Andrews Kurth LLP

Learning from the EU GDPR: What Elements Should the US Adopt?

The current Administration has initiated a process to consider a new comprehensive privacy framework for the United States. In addition, numerous proposals for a federal comprehensive privacy law have been made or are being developed by various groups in the US, including federal legislators. Discussions on what such legislation would look like increased after the entry into force of the European General Data Protection Regulation (GDPR) and the passage of the California Consumer Privacy Act (CCPA). The Centre for Information Policy Leadership (CIPL)[1] believes that in crafting federal consumer privacy legislation, there are specific aspects of the GDPR that US law makers should be aware about. This includes elements which, in CIPL's view, should be incorporated into a new federal US privacy law, as well as elements that CIPL believes require further discussion and adaption for the US context. In effect, our below analysis seeks to promote a basic understanding of useful GDPR concepts and their effective integration into a new US privacy law, such as the risk-based approach to data protection, accountability and good organizational data hygiene practices, but restyled and adapted for the context of US legal and regulatory culture.

As an overarching comment, CIPL believes that any new US privacy law should, consistent with the GDPR, be principles- and risk-based with an emphasis on organizational accountability and the intended outcomes and goals of the law. Any specific obligations should not be overly prescriptive and should provide organizations flexibility in deciding how to meet such requirements and encourage innovative approaches to compliance. The focus should be on what the requirements are; not on how they should be achieved. Such an approach will help ensure the law remains future proof, is scalable for small and medium sized businesses with potentially limited resources and does not unduly stifle data driven innovation.

In addition, a new US federal privacy law should harmonize US privacy legislation, preempting the patchwork of state laws, amending or replacing inconsistent federal privacy laws and preserving well-functioning and materially consistent sectoral laws where appropriate. The benefit of this approach is that it will enable streamlined compliance for covered entities, uniform protection for individuals and competitiveness of the US digital economy and data driven innovation. Harmonization across many jurisdictions was a key goal of the GDPR. Harmonized rules and regulatory processes were much welcomed by multinational businesses operating across the EU Member States and by SMEs who, as a result, now have greater access to the EU wide market. Harmonization was also supported and embraced by policymakers and regulators, who recognized that harmonization would create regulatory efficiencies and benefits to consumers.

Finally, a US privacy law should, as much as possible, be interoperable with other major global privacy regimes and consistent with the 2013 OECD Privacy Guidelines and the 2015 APEC Privacy Framework, which were adopted with the support of the US. This is essential for effective global business and compliance operations of organizations of all sizes. Interoperability relies on creating consistency between the data protection approaches and terminology used in different privacy regimes. At the same time, interoperability should be balanced against the risk of

[1] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 70 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

adopting concepts or approaches that may be ineffective and not in the best interest of businesses, individuals and society in the long run. In other words, interoperability does not necessarily equate to copying other legal regimes or achieving "adequacy" under EU data protection law for the purpose of transferring personal data from the EU to the US.

The following tables outline top aspects of the GDPR which should be incorporated in a new federal US privacy law and top aspects that should not be included without further adaptation. These aspects are stated at a very general level with a non-GDPR expert audience in mind. Each of these aspects would benefit from further explanation, which CIPL would be happy to provide. The content of these short tables is based on the expertise CIPL gained in the course of its GDPR Implementation Project over the past three years, during which we published over 25 white papers and public consultations relating to key GDPR issues and held over 12 GDPR workshops and roundtables with industry representatives and EU data protection authorities.

Top GDPR Aspects to Incorporate *Elements of the GDPR to include in a new federal US privacy law*	
Data Subject Rights ***(Chapter 3 GDPR)***	• The GDPR incorporates a number of individual data protection rights that were already included in the earlier EU Data Protection Directive (e.g. access, correction, objection, erasure) and several novel rights (e.g. data portability, right not to be subject to solely automated decision-making). These rights are not absolute and are subject to exemptions. • Providing individuals with data protection rights empowers them and promotes control over their information. Such rights, coupled with organizational accountability, ensure appropriate protection for individuals, but must be adapted to the US context. • **Recommendation:** Individual rights should be included to empower individuals but these rights should be adapted and modified for the US context, including in light of other competing rights and interests. For example, the right to erasure (sometimes referred to as "the right to be forgotten") must take account of First Amendment rights and interests.
Accountability Principle ***(Art. 24 GDPR)***	• The GDPR includes the accountability principle requiring organizations to (a) put in place policies, procedures and measures implementing the GDPR requirements and (b) be able to demonstrate such implementation. • Accountability promotes responsible data handling by organizations and enables meaningful data protection for individuals through mandating good operational practices that cover the core elements of accountability (e.g. risk assessment, data protection by design, records of processing, implementing security measures, etc.) In other words, accountability puts the burden on organizations rather than individuals, who are often burdened by consent and notice fatigue. • **Recommendation:** Organizational accountability should be included as a building block and essential outcome of any US privacy law. A US law should specify the various commonly accepted elements of organizational accountability to ensure that organizations map their internal privacy programs to all applicable core elements of accountability.
Privacy by Design ***(Art. 25 GDPR)***	• The GDPR requires companies to take account of privacy during the design phase of new products and services and to engineer or design privacy into the development of the product or service. • Privacy by design, together with the elements of organizational accountability and the risk-based approach, constitutes the basis of a modern data privacy framework. • **Recommendation:** Privacy by design should be included in a US privacy law to encourage consideration of data protection issues in the development of new products, services and projects. Such consideration should have regard to the fact that default privacy settings must also be user-friendly and make sense for the product or service concerned.

Risk-based Approach *Accountability obligation (Art. 24 GDPR)* ***Specific obligations based on risk (Art. 25,32,33 GDPR) and high risk (Art. 34-35 GDPR)*** ***Implied consideration of risk (Art. 6(1)(f) and 6(4) GDPR)***	• The GDPR incorporates a risk-based approach, which requires organizations to assess the risks of harm to individuals and the benefits that are associated with the specific uses of personal information and enables risk mitigations that are tailored to the specific risk/benefit assessment. Generally, this approach enables the risk-based calibration and prioritization of compliance measures, thereby facilitating both better privacy protections and more effective use of personal data. • Organizations should have flexibility to determine their own risk assessment methodologies and mitigations. • **Recommendation:** US privacy law should be based on a flexible risk management approach that enables calibration of compliance measures to risks to individuals.
Legitimate Interest *(Art. 6(1)(f) GDPR)*	• The GDPR includes six legal processing grounds or "bases" for using personal data, one of which must be present to validate the legality of the processing. One of these bases is "legitimate interest", which allows processing of personal information where the organization or a third party has a legitimate interest in the processing that outweighs the interests or rights of the individual whose personal information is processed. • This ground for processing is consistent with the risk-based approach to privacy protection in that it requires risk assessments to enable the balancing of interests and rights (e.g. where there is little or no risk of harm to the individual, the outcome of the balancing test is more likely to support the proposed processing of information). • In effect, the legitimate interest ground for processing enables information uses where other GDPR legal bases are not available but the information processing should proceed because the interests promoted by the processing outweigh the interests of the individuals. Where laws include specific legal bases for processing, the legitimate interest basis ensures that the law remains future-proof and able to address previously uncommon or unknown data uses. • **Recommendation:** If a US law incorporates the concept of legal bases for processing it should incorporate a legal basis similar to the legitimate interest balancing test to ensure that all legitimate current and future data uses are enabled through risk/benefit assessments if they are not covered by another legal basis. In the absence of providing for specific legal bases, a US law should still require risk/benefit assessments or a risk-based approach with respect to proposed data uses (as discussed above). The legitimate interest balancing test is a good model for any such risk assessments.
Data Breach Notification *(Art. 33-34 GDPR)*	• The GDPR requires organizations to notify the data protection authority (regulator) of a breach if it is likely to result in a risk to individuals and to notify the individuals themselves if the breach is likely to result in a high risk to such individuals. • The obligation is triggered from the data controller's awareness of a breach and notification must be made without undue delay and, where feasible, within 72 hours of awareness. Where the notification to the supervisory authority is not made within 72 hours, it must be accompanied by reasons for the delay. • All 50 US states have their own breach notification laws each with their own unique requirements as to what triggers a notice and how to report. • **Recommendation:** A US privacy law should harmonize US breach notification requirements by including a simplified and risk-based federal breach notification requirement with a flexible timeframe for reporting that pre-empts the disparate state breach notification laws.

Top GDPR Aspects to Modify Before Incorporation *Elements not to copy directly from the GDPR in a new federal US privacy law*	
Purpose Limitation ***(Art. 6(4) GDPR)***	• The GDPR prohibits using personal data for a purpose other than for which it was originally collected, unless the new purpose is "not incompatible" with the original. • While the purpose limitation principle has the legitimate goal of preventing "free-for-all" data use, its particular approach is becoming obsolete in the data driven society and with the rise of machine learning applications and other emerging technologies. It does not facilitate effective personal data use and reuse that is key for innovation in the economy and should be replaced by other accountability measures that provide the needed controls over the use of personal information. • **Recommendation:** If a purpose limitation principle is included in a US privacy law, it should be coupled with allowing new and future uses of personal information that are "compatible" with, or "not incompatible" with, the original purpose of the collected information. The definition of "compatible" or "not incompatible" uses should be broader than the standard EU interpretation and should allow for future uses that are consistent with, can co-exist with, and do not undermine or negate, the original purpose. This more flexible and permissive approach to new and future uses should include strong accountability-based safeguards, including benefit/risk assessments, to ensure that new uses do not expose the individual to unwarranted increased risks or adverse impacts.
Consent ***(Art. 7 GDPR)***	• Consent is one of the legal grounds or bases for using data under the GDPR. Where relied upon, consent requires a clear, affirmative action by an individual and must be provided for each processing operation or use of personal data. • Opt-in consent is often too burdensome to consumers and results in consent fatigue. Thus, it often undermines, rather than advances, effective privacy protection and disincentivizes user review of notices. • In addition, consent is not appropriate for many data uses. Examples of areas in which consent is inappropriate or ineffective include processing for network security, fraud detection, prevention and investigation or cookie banners, as well as many common uses of data where data processing is necessary to provide a product or service or to comply with a law. • **Recommendation:** To counter consent fatigue, organizations should be encouraged to use consent only where it's a meaningful way to process individuals' data. Consent should be a basis for using data only where consent is appropriate and effective, and where individuals have a genuine choice. Both opt-in (e.g. precise geolocation consent) and opt-out consent (e.g. commercial marketing messages, such as under the CAN-SPAM Act) should be allowed, coupled with appropriate transparency to enable both forms of consent. With respect to data uses where consent is not appropriate or effective, consumers should be protected through other elements of organizational accountability, such as risk/benefit assessments, as described above.

Sensitive Data ("Special Categories" of Data) ***(Art. 9 GDPR)***	• The GDPR prohibits the use of sensitive data (race, ethnic origin, religious or political opinions, trade union membership and genetic or biometric data, health, sex life or sexual orientation) unless an individual has provided his or her explicit consent, or under other limited circumstances. • Restricting the use of certain data by labelling them per se "sensitive" does not ensure appropriate protection for individuals and can have the opposite effect. For example, in the context of AI and machine learning, including sensitive data in the datasets may be necessary to detect and avoid unintended biased and discriminatory algorithmic results. • There may be other categories of data that are equally sensitive in a particular context, such as financial data or location data, depending on their use. Equally, there are many trivial and common uses of ethnicity, political and religious data that are not particularly risky (or "sensitive") whatsoever. • **Recommendation:** The level of sensitivity (and hence risk) and the necessary corresponding protections for certain categories of data (as well as for certain types of data uses) can be captured through a rigorous risk-based approach to all data use activities. In addition, it would be appropriate to require the FTC or other appropriate regulator to provide regulatory guidelines as to what types of personal information and processing activities might be particularly sensitive or risky, which could be rebutted through risk assessments that determine the actual level of risk and the necessary mitigations in a specific context. Such guidelines could draw from and align with existing relevant statutory law, such as anti-discrimination laws. This approach would also avoid the problem of under-inclusive definitions of "sensitive" which sometimes are limited to data that allow for discrimination and do not include certain other data that consumers commonly believe to be sensitive. (For example, the GDPR definition of sensitive data does not include financial data and account numbers).
Notice and Transparency ***(Art. 12,13,14 GDPR)***	• While increased transparency to individuals about what happens with their data is essential for the trusted digital economy, the level of detail required in privacy notices and the amount of technicality prescribed by the GDPR is not achievable or realistic for every data use context (e.g. data transfers, IoT and screenless devices, AI and machine learning applications). • Additionally, too much transparency risks information becoming meaningless to individuals and leads to long and legalistic privacy policies that nobody reads or can act upon. • **Recommendation:** The law should include a minimum transparency requirement (i.e. what data is collected, how is used, with whom it is shared, the consumers' choices and rights and contact details for complaints) but leave flexibility for organizations to provide adequate information depending on the circumstances.

Algorithmic Transparency ***(Art. 13,14,15 GDPR)***	• The GDPR provides individuals with a right to obtain meaningful information about the logic involved in a solely automated decision made about them, where that decision results in a legal effect or a similarly significant effect. • It can be difficult, and sometimes impossible, to meet such a requirement when automated decisions are often made by complex AI algorithms. Moreover, such algorithms are often business proprietary, intellectual property and forced disclosure could undermine competitive advantage and stifle future innovation. • **Recommendation:** A pragmatic approach to "algorithmic transparency" should be based on a broad understanding of "logic involved" and should focus on a useful and actionable level of transparency (including information on whether decisions are automated and what factors they are based on and, where relevant, information regarding the specific algorithmic logic) coupled with appropriate safeguards. These safeguards can include the right to contest the decision or ask for human review of the decision-making if it results in a material negative impact. Of course, not every decision should be subject to scrutiny or human review (e.g. being presented with an ad for a white car instead of a black one), but only those that create a legal effect or harm for individuals (e.g. in the context of insurance, employment and credit).
Solely Automated Decision-Making ***(Art. 22 GDPR)***	• The GDPR introduces restrictive rules for the use of solely automated decision-making that produces legal or similarly significant effects, which, by the data protection regulators in Europe, have been interpreted as prohibited unless certain limited exceptions apply. • These rules do not align well with developing technologies such as AI and machine learning applications. • The concept of what constitutes a "legal or similarly significant effect" is difficult to implement in practice without extensive guidance and clarification and without clearer focus on what harms are to be avoided, such as discrimination. • **Recommendation:** More flexible rules around automated decision-making should apply, with a greater emphasis on organizational accountability measures that can protect individuals more effectively against specifically defined harms, such as unfair discrimination.
Right to Erasure (Right to be Forgotten) ***(Art. 17 GDPR)***	• The GDPR provides for the right to erasure of personal data. • The right to have a company delete data held about an individual is sometimes impossible while the risk to the affected individual is minimal. • In the context of public data mining tools, preventing the collection of further information about an individual requires storing their data in a separate database so the tool knows not to further collect data about the specific individual. In such contexts, personal data cannot be "erased". • In other instances, the right can compromise an entire data operation (e.g. data that is used in clinical trials or to train AI applications, including reducing bias in AI models). • **Recommendation:** Any right to erasure should be defined and implemented in light of other legitimate countervailing rights, interests and practical limitations. The right to erasure should be balanced with the need to retain the data for legitimate reasons, the level of risk of harm to the individual if the data is retained, the impact of the deletion on others and other rights such as the First Amendment. De-identifying the data could be another way to satisfy any right to erasure as it ensures the link to the individual concerned is eliminated.

Controller and Processor ***(Chapter 4 GDPR)*** ***Alternative terms: (Primary Business/ Data User and Service Provider)***	• The GDPR defines certain users of data as controllers and other users as processors, each with their own distinct obligations under the Regulation. • The distinction is in line with the OECD Privacy Guidelines and the APEC Privacy Framework and provides many benefits, including interoperability with other global privacy laws that include the same distinction and, as a result, the streamlining of contract negotiations. However, it also presents some challenges. • For instance, making this distinction among different users of data is becoming increasingly difficult in new digital contexts (e.g. in AI, adtech, blockchain, electronic communications). • **Recommendation:** To the extent the United States implements the controller/processor distinction in a US privacy law, which would be helpful for interoperability purposes, it should take a nuanced approach and ensure that the controller/processor distinction and the requirements imposed upon them are adaptable to the realities of modern data processing, including in contexts where the distinction does not apply or would not make sense. Law makers should consider the accountability model found in laws based on the OECD Privacy Guidelines where each entity is assigned context-based obligations.
Records of Processing ***(Art. 30 GDPR)***	• The GDPR imposes specific and detailed record-keeping requirements on users of personal data regarding all their data use activities. • While understanding what data a company holds is fundamental to organizational accountability, the GDPR requirements are too detailed and extensive, impose unnecessary burdens on organizations (particularly on SMEs) and may lead to tick-the-box compliance for organizations. • **Recommendation:** Documenting data use activities and, in general, understanding the relevance and scope of data use within an organization is an essential part of achieving organizational accountability. A record-keeping requirement should leave flexibility to organizations to devise their own appropriate forms of records management that take into account privacy, security and proprietary considerations.
Data Protection Impact Assessment (DPIA) ***(Art. 35 GDPR)***	• Where a data use is considered to be high risk, the GDPR requires companies to perform a data protection impact assessment (DPIA). • The GDPR itself defines some types of high risk data uses and allows data protection authorities (regulators) to come up with their own lists of additional high risk data uses that would require a DPIA. • Pre-defining "high risk data uses" through a law is ineffective and could be both too broad (capturing uses that are, in fact, not high risk in their specific contexts) or too narrow (by inadvertently omitting apparent low risk or novel uses that may still be high risk in their specific contexts). • **Recommendation:** As privacy risk is contextual, organizations should understand and assess the risks to individuals of all of their data uses. An initial high-level assessment of risk can be aided by guidelines from the FTC or other relevant regulators as to what might be high risk or low risk data uses (such guidelines should be rebuttable by actual risk assessments). Only where likely *high* risks are identified and/or confirmed should organizations have to perform a full-blown DPIA.

Data Transfer Restrictions ***(Chapter 5 GDPR)***	• The GDPR restricts data transfers outside the European Economic Area (EEA) unless (a) the recipient country provides an adequate level of protection (b) there are appropriate safeguards in place for the transfer or (c) an exception for the transfer exists. • This approach to cross-border data protection imposes burdens on efficient data flows. It requires extensive paperwork and formal legal mechanisms that are not necessarily effective in protecting individuals and that drain resources that should be deployed in more important areas of data privacy accountability, compliance and protection for individuals. Cross-border data flows can be protected more efficiently and effectively through other means. • **Recommendation:** A US privacy law should adopt an accountability model for cross-border transfers whereby protections travel with the data. This includes having appropriate privacy and security measures in place and transferring the data in a proper manner, including, for example, through contracts or by participating in cross-border data transfer schemes such as the APEC Cross-Border Privacy Rules (CBPR) or similar accountability schemes.
Fines ***(Art. 83 GDPR)***	• The GDPR empowers European data protection authorities (regulators) to impose fines of up to €20 million or 4% of global turnover for some GDPR violations. • Although the law of the European Union contains safeguards against the excessive use of these powers, a perception exists that GDPR fines can be extraordinary and could wipe out entire businesses which do not make revenues far in excess of €20 million. Such large fines could make companies risk averse, conservative and unwilling to innovate. • **Recommendation:** While penalties and fines can be important, the law should prioritize alternatives to penalties and fining. These can be various forms of constructive engagement and collaboration between regulators and industry to identify potentially problematic products, services and business practices and the ability for regulators to issue orders mandating steps to be taken. Further, fines should be proportionate to the harm, taking into account company size (employees, revenue, profit, etc.), be reduced or mitigated for demonstrated accountability and compliance efforts, and should only be a last resort to deal with negligence, willful or systematic failures. Accountability and proactive compliance should be incentivized by law makers and regulators.

We hope the above will prove useful to US law makers as they consider comprehensive federal privacy legislation for the United States. If you have any questions or would like additional information about any of the above issues, please contact Bojana Bellamy, bbellamy@huntonAK.com; Markus Heyder, mheyder@huntonAK.com; Nathalie Laneret, nlaneret@huntonAK.com; or Sam Grogan, sgrogan@huntonAK.com.