THE EFFECT OF THE EUROPEAN UNION (EU) GENERAL DATA PROTECTION REGULATION (GDPR) ON THE GAMING INDUSTRY

*Zaniah Jordan**

INTRODUCTION

> "Data is the pollution problem of the information age, and protecting privacy is the environmental challenge." Bruce Schneier[1]

Growing concerns about data protection have forced governments to act.[2] Both individual and organizational concerns for personal data protection stem from the various cyber-attacks, data manipulation, malware, everyday hackers, and the like.[3] In an effort to protect citizens personal information "[p]rivacy laws are changing to address the real and perceived risk of harm resulting from the under- or unregulated data" industry.[4] For the first time, data protection laws are "starting to catch up with the extent of personal information being transmitted" and organizations are finding it hard and costly to comply.[5] The European Union ("EU") took the lead in the effort to protect an individual's personal data when it implemented the General Data Protection Regulation ("GDPR").

The European Union Charter of Fundamental Rights states that every EU citizen has the right to the protection of their personal data concerning him or her.[6] In order to enforce this right, the European Commission ("EC") adopted the Data Protection Regulation ("DPR") that aimed to protect individuals with

---

*Zaniah Jordan is a May 2020 Juris Doctorate Candidate at the University of Nevada, Las Vegas, William S. Boyd School of Law, and the Managing Editor of the UNLV *Gaming Law Journal*. Special thanks to my parents Victor and Shana Clanton for encouraging me throughout this process, to Ariana for showing me the value of being a part of something bigger than myself, and to everyone on the Gaming Law Journal for their work on this article and for making my experience on the Journal so wonderful.

1 Bruce Schneier is an internationally renowned security technologist, called a "security guru" by THE ECONOMIST. *About Bruce Schneier*, SCHNEIER ON SECURITY, https://www.schneier.com/blog/about/ (last visited Mar. 6, 2020); BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 238 (2015).

2 Carole Piovesan, *How Privacy Laws are Changing to Protect Personal Information*, FORBES (Apr. 5, 2019, 8:58 PM), https://www.forbes.com/sites/cognitiveworld/2019/04/05/how-privacy-laws-are-changing-to-protect-personal-information/#1b754d51753d; Devon Milkovich, *15 Alarming Cyber Security Facts and Stats*, CYBINT (Sept. 23, 2019), https://www.cybintsolutions.com/cyber-security-facts-stats/.

3 *See* Milkovich, *supra* note 2.

4 Piovesan, *supra* note 2.

5 Tara Seals, *GDPR: True Cost of Compliance Far Less Than Non–Compliance,* INFOSECURITY (Dec. 12, 2017), https://www.infosecurity-magazine.com/news/gdpr-true-cost-of-compliance/.

6 Charter of Fundamental Rights of the European Union, art. 8, 2012 O.J. (C 326/02) 397 [hereinafter Charter of Rights].

regard to the processing of personal data and the free movement of such data.[7] The EC recognized that vast technological advances significantly altered the way personal data was collected around the world.[8] It wanted to take "an essential step to strengthen individuals' fundamental rights in the digital age and facilitate business by clarifying rules for companies and public bodies in the digital single market."[9] To achieve this goal, in 2016, the European Union adopted the GDPR which aims to protect "natural persons with regard to the processing of personal data and the…free movement of personal data."[10] The GDPR took effect on May 25, 2018, enforceable in all EU member states and effectively repealing Directive 95/46/EC.[11]

Unlike its predecessor, the GDPR covers a comprehensive body of data protection regulations such as: additional data subject rights, broader territorial scope, additional obligations and liabilities, and higher regulatory and administrative fines for violators.[12] The GDPR offers extensive additions to the protection of personal data which allow for more organizations to be carefully regulated under the new data privacy rules.[13] Although the GDPR is grounded in EU law, its' scope expands to the United States and other outside countries.[14] Article 3 of the GDPR defines the law's territorial scope and makes clear that the law regulates companies inside and outside EU that track the data of EU residents.[15]

This note will discuss data protection laws in the EU and in the United States and how they relate to the gaming industry. This discussion aims to assist gaming companies in understanding and comparing the relevant provisions of the GDPR and U.S. data protection laws such as, the California Consumer Protection Act (CCPA) and Nevada Data Protection Laws,[16] to ensure compliance with all

---

7 Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31–32 [hereinafter Directive].

8 *Data Protection in the EU*, EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en (last visited Mar. 6, 2020) [hereinafter Guide].

9 *Id.*

10 Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, 3 (EU) [hereinafter the GDPR].

11 Guide, *supra* note 8.

12 Fieldfisher LLP, *General Data Protection Regulation (GDPR),* LEXISPSL, https://advance.lexis.com/api/permalink/071402dc-9827-44f8-b88a-26de03c0daa7/?context=1000522 (last updated June 13, 2019).

13 *Id.*

14 Felix Sebastian, *GDPR in the US: Requirements for US Companies,* TERMLY (June 21, 2019), https://termly.io/ resources/articles/gdpr-in-the-us/.

15 *Id. See also* GDPR, *supra* note 10, at art. 3, 32–33.

16 Nevada data protection laws are relevant because of how data protection laws burden the gaming industry. Nevada Gaming Regulations and Rules will be

pieces of legislation. The discussion will be divided into four parts: (1) GDPR: Scope, and Responsibilities, (2) U.S. Data Protection Laws, (3) Data Privacy Laws Potential Conflicts with the U.S. Gaming Industry, and (4) Strategies for Compliance.

I. GDPR: SCOPE, PRINCIPLES, RESPONSIBILITIES

In order to understand the effect the GDPR has on global personal data protection, it is important to understand who the Regulation protects and what the Regulation regulates. The EU recognized how fast technology allows entities to collect and share personal data and promulgated rules to ensure EU citizens have a high level of protection of such data.[17]

A. Scope and Principles

Every EU citizen has the right to the protection of personal data concerning him or her.[18] The GDPR classifies 'personal data' as "any information that relating to an identified or identifiable" living individual, referred to as a 'data subject.'[19] For example, a user of a website[20] is considered a 'data subject' and if the website owner collects the users name, home address, email address, identification card number, location data, Internet Protocol (IP) address, bank details, or medical information, this is considered personal data.[21] Additionally, a compilation of personal data collected by entity that can lead to identification is also considered personal data. [22] Lastly, the method of the collection of personal data, regardless of the technology used, is still protected by the GDPR. Thus, any collection of personal data that is identifiable, meaning not anonymous or encrypted, is protected by GDPR.[23]

The GDPR has also designated "[s]pecial categories of personal data include[ing] the processing of genetic and/or biometric data where the purpose is to uniquely identify the data subject"[24] and information like race or sexual orientation.[25] For example, facial recognition and fingerprinting,[26] which many

---

exclusively used to show the implications of the GDPR and other state data protection regulations. The Nevada Gaming Regulations are the leading regulatory structures for the gaming industry.

17 GDPR, *supra* note 10, at 2.

18 *Id.* at 1.

19 *Id.* at 33.

20 *Id.* at 6, 11.

21 *What is Personal Data?*, EUROPEAN COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en (last visited Apr. 8, 2020).

22 *Id.*

23 *Id.*

24 Fieldfisher LLP, *supra* note 12*; see also* GDPR, *supra* note 10, at 38.

25 *See* GDPR, *supra* note 10, at 38.

26 Fieldfisher LLP, *supra* note 12, at 37.

casinos and gaming entities in the United States are beginning to implement for added security regulation,[27] would be considered "special data" under the GDPR.

The GDPR broadly expands the rights of data subjects. These rights include: a requirement that organizations provide individuals with information on how their personal data will be used, individuals access to personal data held by an organization, the right to rectification, the right for their data to be erased, the right to object to their personal data being used for marketing purposes, the right to place specific restrictions on the processing of their data, data portability, and the right to request that decisions based on non-human automated processing based on an individual's personal data be limited to human beings only.[28] Ultimately, the GDPR increases the obligations of companies to protect individuals' personal data by requiring transparency.[29]

Allowing EU citizens to have this much control over their personal data "is an essential step to strengthen individuals' fundamental rights in the digital age."[30] The expansive scope of what personal data constitutes will require organizations to examine the data they process and determine whether they are subject to the GDPR or have additional responsibilities under it.[31]

Article 3 of the GDPR defines its territorial scope. The GDPR regulates any entity established in the EU that processes personal data as part of its "core" daily activities, regardless of where the data is processed. Moreover, the GDPR regulates any entity established outside the EU offering goods or services or monitoring the behaviors of EU residents.[32] Data processing is defined as "any

---

[27] Alex Temblador, *Las Vegas Casinos Are Introducing Facial Recognition Technology,* TRAVEL PULSE (Oct. 13, 2018, 11:54 AM), https://www.travelpulse.com/news/hotels-and-resorts/las-vegas-casinos-are-introducing-facial-recognition-technology.html.

[28] GDPR, *supra* note 10, Recital 39, at 7. (for a FN at "how their personal data will be used")*Id*. Recital 58, at 11. (for a FN at "individuals access to personal data held by an organization); *Id.* Recital 59, at 11. (for FN at "the right to rectification" and "the right for their data to be erased"); *Id.* Recital 70, at 13. (For a FN at "the right to object to their personal data being used for marketing purposes"); *Id.* Recital 70, at 13. (For a FN at "the right to place specific restrictions on the processing of their data"); *Id.* Recital 73, at 14. (For a FN at "data portability"); *Id.* Recital 71, at 14. (For a FN at "and the right to request that decisions based on non-human automated processing based on an individuals personal data be limited to human beings only)

[29] *See* Sean McGuinness & Katie Fillmore, *The Impact of GDPR on Attorneys and Law Firms in the United States*, AM. GAMING L. 17–19 (2018); *see* also Katie Thompson, *How GDPR Affects the Online Gambling Industry*, ONLINEBINGO (July 25, 2019, 8:52 AM), https://onlinebingo.co.uk/guides/how-gdpr-affect-online-gambling.

[30] Guide*, supra* note 8.

[31] *See* Fieldfisher LLP, *supra* note 12.

[32] *Rules for Business and Organizations*, EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/who-does-data-protection-law-apply_en [hereinafter *Rules*].

operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption…."[33] Examples relevant to the gaming industry may include, sending promotional emails, storing a user's IP or MAC addresses, video recording (CCTV), access to or consultation of contacts database containing a person's personal data, or even personal employee information used for payroll.[34] Thus, if the data processing falls within the territorial scope of the GDPR as defined by Article 3 then all provisions of the Regulation apply to such data processing.[35]

The GDPR does not apply "to data processed by an individual for purely personal reasons or for activities carried out in one's home, provided there is no connection to a professional or commercial activity."[36] For example, if a person uses his or her own personal contacts to invite friends via email to a party to which he or she is hosting, the GDPR would not apply.[37] This is known as the "household exception."[38] Additionally, the GDPR does not regulate internal data concerning companies or any other legal entities.[39] But it does regulate all personal data "relating to natural persons in the course of a professional activity, such as the employees of a company/organisation, business email address…or…telephone numbers."[40] Thus, any entity that processes the personal data of EU resident consumers, patrons, or users, in a professional or nonprofessional setting, is required to comply.[41]

The GDPR also places specific restrictions on the "type and amount of personal data a company/organisation may process…."[42] These restrictions depend

---

[33] GDPR, *supra* note 10, at 33.

[34] *What Constitutes Data Processing?*, EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_en (last visited Apr. 8, 2020).

[35] *See* EUROPEAN DATA PROTECTION BOARD, GUIDELINES 3/2018 ON THE TERRITORIAL SCOPE OF THE GDPR (ARTICLE 3) (Nov. 2018), https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_3_2018_territorial_scope_en.pdf.

[36] *What Does the General Data Protection Regulation (GDPR) Govern?*, EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_en (last visited Apr. 8, 2020).

[37] *Id.*

[38] *Id.*

[39] *Do the Data Protection Rules Apply to Data About a Company?*, EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-data-protection-rules-apply-data-about-company_en (last visited Apr. 8, 2020).

[40] *Id.*

[41] Katie A. Fillmore, *What is GDPR and How Does it Impact American Businesses?*, BUTLER SNOW: PRODUCT LINES BLOG (June 5, 2018), https://www.butlersnow.com/2018/06/what-is-gdpr-and-how-does-it-impact-american-businesses/.

[42] *What Data Can We Process And Under Which Conditions?*, EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-

on the reason an organization is processing the personal data and what the organization wants to use the data for after it processes it.[43] Several significant principles govern the type and amount of personal data an organization may process.[44] These include lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, compatibility, storage limitation, and integrity and confidentiality.[45] For example, to run a consulting agency and obtain a client's personal data you "should explain in clear and plain language why you need the data, how you'll be using it, and how long you intend to keep it."[46] These principles reflect the GDPR's goal to protect personal data through means of transparency.

B. Responsibilities of Controllers and Processors

Consistent with the purpose of increasing the rights of EU citizens control over their personal data and creating uniform data processing regulations, "the GDPR creates clear lines of accountability over data processing."[47] The GDPR delegates responsibilities between "controllers" and "processors" for the handling of personal data.[48] The provisions "expands significantly upon the controller's responsibility for processing activities and sets out specific rules for allocating responsibility between the controller and processor."[49] Additionally, the Regulation provides guidance for entities carrying out processing activities, relevant to EU residents, outside of the EU.[50] A detailed look into the responsibilities of controllers and processors within and outside the EU will help guide entities on the most efficient way to become GDPR compliant.[51]

Article 3 defines the territorial scope of the Regulations and may provide helpful compliance guidance for both controllers and processers.[52] A controller is 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."[53] Ultimately, a controller determines the reason

---

organisations/principles-gdpr/what-data-can-we-process-and-under-which-conditions_en (last visited Apr. 8, 2020).

43 *Id.*

44 *Id.*

45 *Id.*

46 *Id.*

47 Anna Myers, *Top 10 Operational Impacts of the GDPR: Part 7- Vendor Management*, IAPP (Feb. 4, 2016), https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-7-vendor-management/#.

48 *Id.*

49 *Id.*

50 EUROPEAN DATA PROTECTION BOARD, *supra* note 35, at 3–4.

51 *Id.* at 9–10.

52 *Id.* at 3.

53 GDPR, *supra* note 10, at 33.

personal data is collected and how personal data will be used.[54] They collect and distribute data as they see fit, they modify how data will be used, and determine how long personal data is kept.[55] Controllers also bear the burden of ensuring all data "processing activities are performed in compliance with the Regulation."[56] Controllers bear this burden even when controllers allow third parties to process personal data in a way prescribed by them.[57] This means controllers must implement appropriate technological and organizational measures to ensure the protection of personal data being processed, regardless of where the processing took place.[58] Examples of such protections may include "encryption of personal data" and "regular security testing" or even updating a consumer privacy policy.[59] Controllers' broad responsibility to safeguard personal data places the bulk of responsibility on them as it relates to individuals rights for data protection. For example, safeguarding personal data includes how to deal with a data subjects right to erasure, reporting and notice requirements, breach notification, and maintaining records that show all processing activities.[60] These duties are not displaced when a controller allows a third-party processor to process the personal data on their behalf.

A data processor's duty is dependent on the controller's authority. A data processor is defined as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."[61] This means that processors handle personal data at the sole direction of the controller.[62] A processor may turn into controller status if he or she acts outside of the scope of authority given by the controller when processing personal data.[63] Thus, it is critical when controllers choose a processor, they choose a third-party who can reasonably guarantee they will follow the technological and organization data protection safeguards implemented by the controller in order to comply with the GDPR.[64] This is usually done through a contract between the controller and the processors that lays out the responsibilities compliant with the GDPR.[65]

---

54 Chris Brook, *Data Controller vs. Data Processor: What is the Difference*?, DIGITAL GUARDIAN (Jan. 8, 2020), https://digitalguardian.com/blog/data-controller-vs-data-processor-whats-difference.

55 *Id.*

56 Myers, *supra* note 47.

57 Brook, *supra* note 54.

58 Detlev Gabel & Tim Hickman, *Chapter 10: Obligations of Controllers – Unlocking the EU General Data Protection Regulation*, WHITE & CASE (Apr. 5, 2019), https://www.whitecase.com/publications/article/chapter-10-obligations-controllers-unlocking-eu-general-data-protection.

59 *Id.*

60 Myers, *supra* note 47.

61 GDPR, *supra* note 10, at 33.

62 Myers, *supra* note 47.

63 *Id.*

64 *Id.*

65 *Id.*

Article 28 lays out additional processor duties separate from contractual obligations with the controller.[66] These duties include (1) processing data only as instructed by controllers; (2) using appropriate technical and organizational measures to comply with the GDPR; (3) deleting or returning data to the controller once processing is complete; and (4) submitting to specific conditions for engaging other processors.[67]

Because processors conduct processing activities under the strict discretion of controllers, they are also restricted from hiring a sub-processor to carry out the request of the controllers.[68] However, processors may enlist another processor with prior specific or general written permission of the controller.[69] Controllers ultimately decide whether they will allow for additional processors.[70] Both controllers and processors play a vital role in GDPR compliance. Controllers are always responsible for damages caused by processing personal data that violates the individual rights under the GDPR.[71] However, if a company is clear on the roles of the controller and processor under the GDPR it can significantly reduce the risk of data exposure in violation of the Regulation.[72] Accordingly, companies should reassess their third-party vendor agreements to achieve compliance.[73]

C. Legal Basis for Data Processing

Article 6 of the GDPR provides six legal bases for when a company may process personal data.[74] One or more of these legal bases must be met in order for a company to process personal data.[75] The six options include the following:

(1) **Consent**: If a data subject provides express consent for their personal data to be processed by the controller then a company may process such data. Consent "must be exclusive, reflective of a data subjects' discretionary action, a positive and freely given response to a well-structured, unambiguous description of the processing activity."[76] Therefore, a controller must be able to prove consent was

---

66 *Id*; *see also* GDPR, *supra* note 10, at 49.
67 Myers, *supra* note 47.
68 *Id.*
69 *Id.*
70 *Id.*
71 *Id.*
72 Brook, *supra* note 54.
73 *See id.*
74 *See* GDPR, *supra* note 10, at 36.
75 *When Can Personal Data Be Processed?,* EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/when-can-personal-data-be-processed_en (last visited Apr. 8, 2020).
76 Ivan Klekovic, *Is Consent Needed? Six Legal Bases to Process Data According to GDPR*, EU GDPR ACADEMY,

given.[77] For organizations, consent as a legal basis may be unfavorable because the GDPR places strict requirements for "validity of obtaining and managing consent."[78] Moreover, the GDPR mandates that consent can be withdrawn at any time at the request of the data subject.[79] This is especially burdensome when companies collect data for marketing purposes.[80] In this instance, consent is mandatory under the GDPR.[81]

(2) **Compliance with a legal obligation**: A company may process data in order to meet EU law or regulations.[82] An example of this type of data processing may be reporting problem gambling in compliance with gaming regulations or reporting personal data for public safety.[83]

(3) **Contractual Performance**: Personal data may also be processed if it is required to carry out a contractual obligation between a company and a client.[84] This type of legal basis may occur when parties are attempting to enter an agreement, complete an existing agreement, or prior preparation in anticipation of an agreement or negotiation.[85] For example, "processing credit card details in order to perform payment."[86] An example where a contract does not yet exist occurs "when an individual requests information from a service provider about a particular service via e-mail or social network, the processing of that individual's personal data is permitted for the purposes of responding to the inquiry."[87]

(4) **Public Interest**: Personal data may be processed if "necessary for the performance of a task carried out in the public interest under EU law or national legislation."[88] An example may include processing information for the purposes of tax information.

---

https://advisera.com/eugdpracademy/knowledgebase/is-consent-needed-six-legal-bases-to-process-data-according-to-gdpr/ (last visited Apr. 8, 2020).

77 *Id.*
78 *Id.*
79 *Id.*
80 *Id.*
81 *Id.*
82 *When Can Personal Data Be Processed?*, *supra* note 75.
83 *See id.*
84 *Id.*
85 Klekovic, *supra* note 76.
86 *Id.*
87 *Id.*
88 *When Can Personal Data Be Processed?*, *supra* note 75.

(5) **Vital Interest**: Personal data may be processed if it is necessary to protect a vital interest of a data subject.[89] This usually occurs in an emergency situation involving life or limb.[90]

(6) **Legitimate Interest**: The broadest legal basis under the GDPR is the principle of "legitimate interests."[91] This principle allows companies to process data so long as it has a "legitimate interest" that does not infringe on the "fundamental rights and freedoms of the person whose data" is being processed.[92] Therefore, controllers must use a balancing test to determine whether a company's legitimate interest significantly affects the rights of individuals.[93] However, a person's individual rights always trumps a company's legitimate interest.[94] An example of an legitimate interest would be if a company monitors the use of its employees network devises to protect the personal data of individuals.[95] Processing of personal data would be appropriate in this instance so long as the "least intrusive method" of monitoring is chosen (limiting an employee's accessibility of certain websites).[96]

As we have already begun to see, the GDPR has significantly increased companies data privacy obligations.[97] As an incentive to comply, the GDPR also significantly increased the penalties for breach.[98] For example, infringements for certain provisions could potentially result in penalties of up to 10,000,000 euros, and non-compliance administrative fines of up to 20,000,000 euros.[99]

The GDPR provides expansive protections for an individual's personal data rights. The Regulations provide a uniform regulatory framework that identifies specific rights of data subjects and the responsibilities of companies in order to meet the compliance requirements under the Regulation.

---

89 *Id.*
90 *See id.*
91 Klekovic, *supra* note 76.
92 *When Can Personal Data Be Processed?*, *supra* note 75.
93 Klekovic, *supra* note 76.
94 *When Can Personal Data Be Processed?*, *supra* note 75.
95 Klekovic, *supra* note 76.
96 *When Can Personal Data Be Processed?*, *supra* note 75.
97 McGuinness & Fillmore, *supra* note 29.
98 Simona Chirica*, The Main Novelties and Implications of the New General. Data Protection Regulation.*, 6 PERSP. BUS. L. J., 159, 173 (2017).
99 *Id.*

II. U.S. DATA PROTECTION LAWS

A. United States Federal Government Data Protection Laws

Like the EU, the United States realized the impact technology has on the collection of personal data and shared similar concerns regarding the legal protection of such data.[100] The United States has several federal and state specific laws regarding the data protection of individuals.[101] Although national data protection has become a pressing concern for the U.S. Federal Government, current legislation and laws regarding data privacy "are complex and technical, and lack uniformity."[102] Consequently, the current U.S. Federal data protections laws are not as uniform and concise as the GDPR.[103] Although the constitutional "right to privacy" has developed with the expansion of technological advances, the right "generally guard[s] only against government intrusions and [does] little to prevent private actors from abusing personal data online."[104] Federal statutes also protect individuals' personal data or cybersecurity.[105] These include the Children's Online Privacy Protection Act, the Communications Act, Video Privacy Protection Act, Electronic Communications Privacy Act, Computer Fraud and Abuse Act, the Consumer Financial Protection Act, and others.[106] However, these statutes do not protect the processing and using of personal data by the private sector as they regulate specific industries and categories of data.[107]

Because the U.S. Federal Government does not provide specific safeguards of personal data to individuals some states have enacted their own data protection laws.[108] Similar to the GDPR, some state privacy laws regulate all forms of personal data, such as the California Consumer Privacy Act (CCPA),[109] while other states, such as Nevada, data privacy protections are just as limited as U.S. Federal government data protection laws.[110] Proponents of more uniform privacy laws argue "that Congress should consider creating similar protections in federal

---

100 CONGRESSIONAL RESEARCH SERVICE, DATA PROTECTION LAW: AN OVERVIEW 1 (Mar. 25, 2019), https://fas.org/sgp/crs/misc/R45631.pdf.

101 DLA PIPER, DATA PROTECTION LAWS OF THE WORLD: UNITED STATES 2 (Jan. 27, 2020), https://www.dlapiperdataprotection.com/index.html?t=law&c=US&c2=GB.

102 CONGRESSIONAL RESEARCH SERVICE *supra* note 100, at 1.

103 For a comparison of data protection laws between the US and the European Union see DLA Piper, Data Protection Laws of the World (last visited Mar. 23, 2019), https://www.dlapiperdataprotection.com/index.html?t=law&c=US&c2=GB.

104 *See* CONGRESSIONAL RESEARCH SERVICE *supra* note 100, at 2.

105 *Id.*

106 *Id.*

107 *Id.* at 2.

108 *Id.*

109 *Id.*

110 *See* discussion *infra* Section III.C.

law."[111] Conversely, others have criticized data protections laws similar the GDPR "as being overly prescriptive and burdensome."[112]

B. California Consumer Privacy Act

Similar to the GDPR, the California Consumer Privacy Act (CCPA) "aim[s] to guarantee strong protection for individuals regarding their personal data and apply to businesses that collect, use, or share consumer data, whether the information was obtained online or offline."[113] The CCPA is very similar to the GDPR in regard to individual rights of data subjects; however, the CCPA differs in scope of application, collection limitations, and controller and processor obligations.[114] For example, the GDPR provides specific obligations for controllers regarding the processing of personal data, while the CCPA does not.[115] Also, the CCPA does not follow the same "legal basis" requirement for data processing that the GDPR does.[116]

Similar to the GDPR, the CCPA focuses on "transparency obligations"[117] between the controller and the consumer. However, the CCPA specifically focuses on limiting the "selling of personal information, requiring a 'Do Not Sell My Personal Information' link to be included by business on their homepage."[118] The CCPA also considers third-party data processors obligations and safeguards a consumers data that is inappropriately being processed based on the agreement with the controller at the time the personal data was collected.[119] Ultimately, the CCPA grants individuals the following data protection rights: the right to know what personal information is being collected about them, the right not to be discriminated against for exercising a privacy right under the Act, the right to know who their data is being sold to, the right to opt out of those sales and the right to delete previously collected data.[120]

---

111 CONGRESSIONAL RESEARCH SERVICE *supra* note 100, at 1.

112 *Id.*

113 ALICE MARINI ET AL., COMPARING PRIVACY LAWS: GDPR V. CCPA, https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf.

114 *Id.*

115 *Id.*

116 *Id.*

117 *Id.*

118 *Id.*

119 MARCINI ET AL., *supra* note 113.

120 Thomas Germain, *California's Privacy Law is Finally Here. Now What?*, CONSUMER REPORTS (Jan. 2, 2020), https://www.consumerreports.org/privacy/california-privacy-law-ccpa-california-consumer-privacy-act/; *see also* CALIFORNIA DEPARTMENT OF JUSTICE, CALIFORNIA CONSUMER PRIVACY ACT FACT SHEET, OFFICE OF THE ATTORNEY GENERAL (last visited Mar. 12, 2020), https://oag.ca.gov/system/files/attachments/press_releases/CCPA%20Fact%20Sheet%20%2800000002%29.pdf.

The CCPA regulates the processing of all personal data.[121] Its broad definition defines personal information as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[122] The CCPA gives examples of personal information.[123] For example, biometric information, geolocation, electronic network activity such as browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement, commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies and any inferences drawn from any of the information a consumer provides that is protected by the Act.[124]

The CCPA applies to any business doing business in California, that collects the personal information of California residents, has a gross annual revenue in excess of $25 million, buys, receives, or sells the personal information of 50,000 or more consumers, households, or devices, and is for profit.[125] Additionally, businesses that process the personal information of more than four million individuals will be subject to additional regulations.[126] Whether or not the CCPA applies to business outside of California that process personal data of California consumers, such as third-party processors, is still undetermined.[127] Until California gives guidance on how "doing business" is defined it would be helpful for companies to look at how other California statutes have defined "doing business."

Like the GDPR, the CCPA provides money damages for violation of the Act.[128] Damages depend on the type of violation, but a penalty can result in fines up to $2,500 for each violation and $7,500 for an intentional violation.[129] Although not identical to the GDPR, the CCPA expands the data protection of individual residents of California and provides a regulatory scheme that holds companies responsible for the way in which they process personal data.

---

121 CALIFORNIA CONSUMER PRIVACY ACT FACT SHEET, *supra* note 120.

122 CAL. CIV. CODE § 1798.140(O)(1) (2018).

123 CONGRESSIONAL RESEARCH SERVICE *supra* note 100, at 38.

124 CAL. CIV. CODE § 1798.140(O)(1)(A)-(K) (2018).

125 *Id.; see also*, CAL. CIV. CODE § 1798.140(c)(1) (defining "business" as any company with more than $25 million in annual gross revenues, or that engages in the buying, selling, or receipt of the personal information of 50,000 or more California residents, or that derives more than 50% of its annual revenues from the sale of California residents' personal information).

126 CALIFORNIA CONSUMER PRIVACY ACT FACT SHEET, *supra* note 121.

127 *See* CONGRESSIONAL RESEARCH SERVICE, *supra* note 100, at 38.

128 MARINI ET AL., *supra* note 113, at 37.

129 *Id.*

C. Nevada Data Privacy Laws

Just like the EU and California, Nevada has also enacted data protection regulations.[130] The SB 220 functions as an amendment to existing privacy regulations in the state.[131] Nevada's law requires operators of websites and online services to inform consumers how their data will be used and allow them to opt out of the sale of such information to another party.[132] An operator is defined as any person or entity that:

> a) owns or operates an Internet website or online service for commercial purposes;
> b) Collects and maintains covered information from consumers who reside in Nevada and use or visit the Internet website or online service; and
> c) Purposefully directs its activities toward this State, consummates some transaction with this State or a Resident thereof, [or] purposefully avails itself of the privilege of conducting activities in this State.[133]

The definition of operator has a broad scope similar to the GDPR in that it does not limit operators (or controllers) of websites to those who operate only in Nevada. However, the scope is limited to online internet operators only, unlike the CCPA which includes online and offline business websites.[134]

Additionally, SB 220 is similar to the GDPR and the CCPA in that it protects a wide range of information. The following types of information are covered by the law: first and last name, home address, email address, telephone number and social security numbers, and inferences that can be made about a person through a compilation of collected information.[135] Moreover, SB 220 gives consumers the right to request their personal data not be sold to third-party operators. An

---

130 Grant Gross, *Nevada Latest State to Pass Data Privacy Law*, WASH. EXAMINER (Oct. 10, 2019), https://www.washingtonexaminer.com/policy/nevada-latest-state-to-pass-data-privacy-law.

131 *Id.*; Chris Brook, *Nevada Beats California With New Privacy Law*, DIGITAL GUARDIAN (Oct. 7, 2019), https://digitalguardian.com/blog/nevada-beats-california-new-privacy-law.

132 Gross, *supra* note 130.

133 Brook, *supra* note 131.

134 Alexandra Scott & Lindsey Tonsager, *Nevada's New Consumer Privacy Law Departs Significantly From The California CCPA,* COVINGTON & BURLING LLP: INSIDE PRIVACY (June 10, 2019), https://www.insideprivacy.com/united-states/state-legislatures/nevadas-new-consumer-privacy-law-departs-significantly-from-the-california-ccpa/.

135 Brook, *supra* note 131.

operator must acknowledge this request within 60 to 90 days, so long as the operator can reasonably prove this request is made by the consumer.[136]

Overall, the scope of SB 220 is narrower than both the GDPR and the CCPA.[137] Although it does require an internet operator to post a "Do not sale" link it does not require the link to be clearly identifiable by the consumer.[138] The penalties under SB 220 are capped at $5,000 per violation.[139]

III. POTENTIAL CONFLICTS BETWEEN DATA PRIVACY LAWS AND THE U.S. GAMING INDUSTRY

Amongst the several data protection laws previously discussed, it is apparent that the GDPR possesses the broadest scope and strictest rules as it pertains to data protection.[140] However, there are several rights that data protection laws have in common. These are the right to erasure (or the right to opt-out), the right to restriction of process, increase general consent, requirements, transparency notifications, breach notifications, and purpose limitations. While perfecting data protection compliance in the EU and U.S. is no small feat, gaming companies would be wise to comply with the GDPR, as the Regulations possess broad scope and the most stringent form of data protection. Accordingly, several internal steps may be taken in order to increase odds of GDPR compliance.There are several considerations gaming entities should bear in mind while becoming compliant.

A. Consent

Consistent with the purpose of the GDPR of expanding consumer rights companies should aim to achieve customer consent. The GDPR requires companies to expressly inform customers that their personal data is being collected and why and how that data will be used. The request for consent needs to be in plain language and easy for customers to understand.[141] Although silence or disinterest from the customer used to pass as consent, the GDPR now requires more "as companies need to be able to prove that they received approval from customers to use their information."[142] Even more so the terms of the customer consent notice must reflect the customers most up-to-date information and the purpose for which their personal data is being used. Should this purpose change, companies would need to issue a new customer consent request. This means that if the

---

136 *Id.*

137 *Id.*

138 *Id.*

139 *Id.*

140 *See supra*, Section I.

141 Manuel Grenacher, *GDPR, The Checklist for Compliance*, FORBES (June 4, 2018, 7:00 AM), https://www.forbes.com/sites/forbestechcouncil/2018/06/04/gdpr-the-checklist-for-compliance/#367ab7c5bec7.

142 *Id.*

purpose for the customers' personal data being collected changes, that data may not be used for the new purpose. Lastly, to ensure customer rights, companies should respect the right to be forgotten, and inform customers of that right. At any time, a customer may request to have his or her personal data withdrawn. This means that companies will have to timely respond to that request by a complete removal of that customer's personal information and inform the customer once the removal is complete. [143]

All data protection laws seemingly have the goal to increase consumer consent. The GDPR has been very clear that a pre-checked box or 'terms and conditions' click wrap swarming with legalese will not suffice in demonstrating a data subject understands why and how their personal information will be used. This may cause gaming entities to have to re-write contracts between consumers that may cause consumers to ask questions before signing or maybe not want to consent at all. For gaming enitites, the luxury of pre-checked boxes or 'terms and conditions' meant quicker transactions. Some may argue that the informed consent regulations will cause consumers to have to be physically notified of their rights and how their information will be used. However, this concern may be misplaced. The GDPR is mostly focused on consumers being able to clearly understand their rights—not who can explain their data privacy rights to them. Thus, so long as gaming entities are able to present a consumer's data protection rights in a clear and concise way and free of legalese, they should not have a problem with complying with consent.

B. Specific Consideration: Player Cards and Casino Comps

Common in the gaming and casino industry are "player cards." Player cards are unique to each customer and allow for easy transfer of funds while gambling in casinos. Customers are encouraged to sign up for player cards in order to potentially receive incentives such as comps,[144] based on their play and other promotional offers.[145] In order to receive a player's card, customers typically need to present valid identification to players card agent. Casinos will use the customer's name, date of birth, home address, email address, gender, driver's license number, the driver's issuance and expiration date, and in some cases even social security number.[146] After the customers are issued their player card, the card will also track how much they wager and how long they typically spend gambling.[147] Additionally, the player card may track where customers use their player card—to eat, to play slot machines, to purchase a room in the casino's hotel, or even if

---

143 *Id.*

144 Chandeni K. Gill, *Patron Data Privacy & Security in the Casino Industry*, 3 UNLV GAMING L. J. 81, 81 n. 1 (2012). (A comp is also known as a complimentary and signifies something given without charge).

145 *Id.* at 81.

146 *Id.*

147 *Id.* at 82.

they request a credit line from the casino. Casinos often then take this information and use it to determine customers gabling habits, and even a "plan to incentivize his return, and an individual profit-and-loss projection by which the casino may gauge its future marketing investment…."[148]

The personal data being collected for players cards triggers the GDPR when collected from EU residents. Casinos readily provide customers with playing cards to create loyalty. The casinos do not want the player to forget the casino once the gambler is finished playing or ends their vacation. The increased transparency of customer consent may slow this phenomenon down. Casinos will no longer be able to hand out players cards so freely. Instead they will have to thoroughly explain how the personal information on the players cards will be used by the casinos. This means explaining tracking behaviors, individualized advertisement schemes, and a player gambling habits. This may or may not sound appealing to customers as more customers are becoming more worried about their personal data being used for unlawful purposes.[149]

The implications of informed consent may be vast. For casinos this may mean less individualized advertising because customers may opt out of their players cards after they are informed how they will be targeted with advertisements. This may also mean less sales for casinos through those individualized ads. Although casinos may be opposed to the extra cost it may take to ensure compliance with the GDPR through advertisements, the easier way for this to be done is through its consent policies and procedures. So long as consumers are informed and genuinely understand that by providing their personal information they may be solicited with advertisements and offers, then casinos should not have a problem with the way they advertise to their consumers. Casinos may, in conjunction with their privacy and marketing department, come up with efficient, but still attractive ways to inform customers about their privacy rights that will not deter them from opting out of consumer products such as player cards.

C. Consumer Safety Transparency

Gaming entities should also consider how the GDPR will affect consumers concern with the safety of their personal data. For the average consumer, ignorance is sometimes bliss. It might frighten consumers if gaming entities keep bringing up personal data and security breach concerns. Consumers may begin to wonder why entities are so adamant about the consumers security and begin to distrust entities based on false perception. Thus, gaming entities should be careful about how they portray their concerns for consumer personal data protection and why they are being careful to ensure consumers understand why they are *only now* thoroughly being told about their rights as a consumer. This creates a higher importance for training at the lower employment levels. This is where training at the basic level will be useful. Employees, such as cashiers, hotel

---

148 *Id.*
149 *Id.*

registrations, call centers, and customers service centers, should be coached on how and what to say to customers when having to disclose personal data privacy rights under the GDPR.

D. Cost of Compliance

The GDPR sets clear responsibilities of both processors and controllers and establish steep fines for those entities that fall short of compliance. This places a high burden on the U.S. gaming industry because it means more money and resources must be spent to make sure they are not fined whether they intentionally violate the Regulation or not. The gaming industry should consider several factors that may cause a rise in cost to ensure compliance.

A very important factor for compliance is education and change in procedure. Although the GDPR is fairly clear on its requirements, a grey area remains when trying to determine the scope of the regulation. Gaming entities will have to not only receive training and update their policies but also the GDPR regulation compliance will require consistent monitoring. This means more resources. Everyone who is involved in collection personal data within a specific gaming entity will have to be trained on best practices in compliance with the GDPR. The resources require to achieve are likely vast, but it is something entities should implement in order to avoid penalties for non-compliance.

Gaming entities should also think about internal governance and responsibility. The GDPR requires that gaming entities be able to show compliance. This will likely require maintaining records of every type of data processing activity including policies and procedures each entity put in place to show compliance. Both data processors and controllers should create a "detailed personal data inventory" so they can make informed decisions on how to best comply with the GDPR and avoid a potential breach. Records that reflect GDPR compliance should remain in effect indefinitely in the event of an audit and be clear as to why these records have been stored for so long. As mentioned above, most entities do not know when a breach will occur so it is important during an investigation for an entity to show they were in compliance and did everything they could to protect their consumers from such a breach.

Companies should also be aware of Article 27 of the GDPR, which states that all non-EU companies who are bound by the GDPR shall designate, in writing, a representative in the Union.[150] On its face, it would seem that compliance with this Article is hard to achieve however, U.S. companies are appointing service firms as their designated representative.[151] This may be an incentive for U.S. companies because they can choose EU service providers who are more familiar with the GDPR and how to comply. The service representative would be

---

[150] GDPR, *supra* note 10, at 48–49.

[151] Fiona Chan, *GDPR Compliance for Non-European Companies and Organizations*, MEDIUM (May 26, 2018), https://medium.com/@fionaschan/gdpr-compliance-for-non-european-companies-and-organisations-c59320cbc091.

"responsible for dealing with the supervisory authorities," which are located in the EU, and the data subject access requests.[152] In addition to adhering to Article 27 of the GDPR, companies should also appoint or hire a Data Protection Officer ("DPO"). A DPO is a person who ensures GDPR compliance and is required for companies larger than ten to fifteen employees that process personal data.[153] A DPO's primary duties are to regularly and systematically monitor data subjects and process large scales of special categories of data.[154] This means the DPO must be well versed in the scope and limitations of the GDPR. The hiring of these types of representatives is crucial to compliance with the GDPR and might be worth the funds in order to avoid the high fees for any GDPR violation.

The gaming industry is highly monopolized. For example, Caesars Entertainment owns several gaming entities across the country.[155] Caesars will have to comply with the GDPR because patrons visit from all over the world. Having a GDPR liaison and a main GDPR department running twenty-four hours is necessary for compliance. Liaisons should be well apt and constantly researching the ways in which the GDPR may apply to any activity by the gaming entity that involves collecting personal data. They should understand policies regarding breach notifications and also handle any consumer request from erasures to general information for clarification of their rights. Having one or two people whose only job is to make sure a gaming entity is in compliance with GDPR can be an efficient way to avoid noncompliance.

E. Impact Assessments for New and Existing Technology

As technology advances and consumers' needs quickly increase, companies often times make quick changes in advertising and product marketing techniques that require personal data from consumers. To be cautious not to violate the GDPR when introducing these new techniques, companies should consider performing a Data Protection Impact Assessment. ("DPIA").[156] If a company permanently stores personal data, it should complete a DPIA on each project that involves the personal data stored.[157] The DPIA is "an audit of [a companies'] own processes and procedures that measures how these processes affect or might compromise the privacy of the individuals whose data it stores, collects or processes."[158] A company's participation in a DPIA may achieve three key things: 1) it can ensure compliance with applicable legal, regulatory, and policy requirements regarding privacy; 2) it can determine the risk and effects, and 3) it will

---

152 *Id.*
153 Grenacher, *supra* note 141.
154 *Id.*
155 CAESARS ENTERTAINMENT, https://www.caesars.com/destinations (last visited Mar. 18, 2020).
156 Grenacher, *supra* note 141.
157 *Id.*
158 *Id.*

help evaluate protections and alternative processes to mitigate potential privacy risks.[159] DPIA's are not only a good way to stay in compliance but also identify unintentional non-compliance that may lead to unwanted breaches and fines. Participating in DPIA's will also help companies assess the effectiveness and need for potential projects by carefully examining the effects it could have on customer communication and trustworthiness.

Although DPIAs are a great way to ensure compliance under the GDPR, it will likely be very costly to gaming entities. Not only would entities have to set up their own system of DPIA's, but they will also have to constantly change and measure their perfection of compliance as new innovations and ideas are presented. Each project or new idea would have to be examined to make sure it is in compliance with GDPR. DPIA's would have to be completed constantly to ensure compliance that may cause a financial burden on gaming entities.

IV. BREACH NOTIFICATION

The GDPR also requires gaming entities to put into place an efficient personal data breach notification system.[160] Controllers must report personal data breaches to lead supervisory authorities with seventy-two hours after becoming aware of the breach and also informing individual who were affected by this breach. With this requirement processors and controllers will need to set up around the clock teams to ensure they are able to identify and react to security breaches in a manner which complies with the requirements of the GDPR.[161]

Another concern that reporting breaches may cause is informing consumers who are outside of the country. Although email is more than likely the quickest way to inform a consumer of breach, time differences may also pose a constraint on breach notifications. But the most efficient way of a breach notification may be an automatic system that notifies gaming entities when there are suspicious activities with regards to personal data. This system would take time to develop but it would have to be capable of identifying common and not so common forms of data breaches. Should the breach be one that triggers a notification to consumers under the GDPR, gaming entities should have a system in place where a quick click or algorithm notifies which consumers may have potentially been breached. This could buy gaming entities time to really assess each breach and determine if additional notification to the consumer is needed, such as a detailed explanation of how the consumers data was breached, what the consequences of the

---

159 *Id.*

160 Matt Middleton-Leal, *GDPR Data Breach Notification: How to Report a Personal Data Loss*, NETWRIX (Apr. 19, 2018) https://blog.netwrix.com/2018/04/19/gdpr-rules-of-data-breach-notification-how-to-report-personal-data-loss-and-avoid-fines/.

161 Detlev Gabel & Tim Hickman, *Chapter 11: Obligations of Processors — Unlocking the EU General Data Protection Regulation*, WHITE & CASE LLP (Apr. 5, 2019) https://www.whitecase.com/publications/article/chapter-11-obligations-processors-unlocking-eu-general-data-protection.

breach may be, and how the entity plans on rectifying the breach. Obviously, this will require extra resources but because gaming entities already have security and compliance teams available that are considering the GDPR, enhancing security will not be so much of a burden.

V. ESTABLISHING A FEDERAL BLANKET DATA PROTECTION SCHEME

Together, the federal government, states, and business entities may be more obliged to work together to create a blanket and uniform system in dealing with GDPR compliance that in the long run would cut cost for all parties who are subject to the GDPR. Compliance would be easier and more efficient if each interested party collectively came together to analyze each part of the GDPR and its obligations, then create regulations and an authority board to report to. This structure would mitigate the cost of compliance by spreading resources and responsibility amongst all entities involved.

The GDPR may potentially initiate a blanket lead authority in data protection that the United States currently does not have. Many casinos serve more than one EU member state, thus the GDPR may cause the states with a high gambling presence and the federal government to work together to create a uniform authority and regulations in order to make it easier to comply. Casinos generally have a vested interest in protecting their consumers and themselves from data breaches. However, the U.S. consumer data protection in the gambling industry is usually regulated at the state level. For example, in Nevada, its state statute defines what personal information is and how it needs to be "collected, maintained, and disseminated."[162] However, this provision is not a part of Nevada's Gaming Control Act, but any business with a gaming license may be subject to its provision. Nevada rationalizes this since the Control Board has the power to regulate the gaming industry as it sees fit.[163]

Gaming Boards and regulators who are more advanced in data protection laws within the gambling industry may find it in their best interest to capitalize on their expertise in gaming regulation and take the lead on creating a blanket regulatory board that would help all gaming entities in compliance with the GDPR. The models could range from federal responsibility which would provide that the government take the lead in determining how and to what extent U.S. entities should comply with the GDPR. This model may be easier when negotiating and discussing compliance with the EU as it may be hard for individual states to do so.

Another option is member-state responsibility that would require states who have allow gaming to come together and figure out a uniform way to comply with the GDPR. This type of governance may be well-suited because states, such

---

[162] Karl Rutledge et al., *Casino Player Clubs & Nevada's Data Protection Requirements,* CASINO ENTERPRISE MGMT. (Dec. 2013), https://www.lrrc.com/files/Uploads/Documents/Rutledge_1213.pdf.

[163] *See* Nev. Gaming Comm'n Reg. § 5.011 (2020).

as Nevada and New Jersey, who have pioneered the gaming industry, may come together with the best ideas for ensuring compliance and even a uniform way to notify the EU of any breaches that should occur. Any collaborative model is the safest and most efficient way to guarantee that the gaming industry complies with the GDPR.

CONCLUSION

The GDPR provides a blanket regulation on personal data of consumers that is used for the everyday functions of corporations. The requirements under the EU, although stringent, provide a good standard for compliance that was not there before. Gaming entities may not like compliance at the front end because the cost to implement new requirements under the GDPR will be costly, but from a fiscal and legal prospective it may be worthwhile. Fiscally the penalties for noncompliance under the GDPR are very high, with potential to reach a million United States dollars. Outside of the penalties financially, a breach could also have legal implications—such as tort actions brought about by consumers who have been harmed by a breach—to bring lawsuits that may cost a company a lot in damages. Additionally, a breach of personal security may also cause reputational loss that can also be fiscally harmful to a company. Thus, non-compliance can do more harm than good.

The more stringent requirements will require several changes in gaming entities' privacy and security structure. While GDPR complinace may require a lot of resources on the front end, increased consumer data protection will not only be benefit the consumer but it will also benefit the entity to be able to properly protect itself from all potential consequences of a breach.