JTC Resource Bulletin

GDPR for US Courts

Version 1.0
Adopted 19 September 2018

Abstract

In May of 2018, new data privacy and security regulations went into effect in the European Union. Overnight, it seems, GDPR-compliance has become “best practice” expectation well beyond the boundaries of the EU. If EU data privacy standards were applied to US courts, the sensitive nature of court data would warrant the most stringent protections. The EU’s legislation is a call-to-action and US courts should have at least a basic understanding of the legislation and a game plan for preparing for similar legislation in the US.

Document History and Version Control

Version	Date Approved	Approved by	Brief Description
1.0	9/19/2018	JTC	Release document

Acknowledgments

This document is a product of the Joint Technology Committee (JTC) established by the Conference of State Court Administrators (COSCA), the National Association for Court Management (NACM) and the National Center for State Courts (NCSC).

JTC Mission:
To improve the administration of justice through technology

Joint Technology Committee

COSCA Appointments
David Slayton (Co-Chair)
Texas Office of Court Administration

David K. Byers
Arizona Supreme Court

Laurie Dudgeon
Kentucky Administrative Office of the Courts

Rodney Maile
Hawaii Administrative Office of the Courts

NACM Appointments
Kevin Bowling (Co-Chair)
Michigan 20th Judicial Circuit Court

Paul DeLosh
Supreme Court of Virginia

Danielle Fox
Circuit Court for Montgomery County, Maryland

Kelly C. Steele
Florida Ninth Judicial Circuit Court

Jeffrey Tsunekawa
Seattle Municipal Court

NCSC Appointments
The Honorable O. John Kuenhold
State of Colorado

The Honorable Constandinos Himonas
Utah Supreme Court

CITOC Appointments
Jorge Basto
Judicial Council of Georgia

Casey Kennedy
Texas Office of Court Administration

Ex-officio Appointments
Joseph D.K. Wheeler
IJIS Courts Advisory Committee

NCSC Staff
Paul Embley

Jim Harris

Contents

Introduction

In May of 2018, new data privacy and security regulations went into effect in the European Union. The General Data Protection Regulation - known more commonly by the acronym GDPR – is a set of rules for the protection of personal data. The law applies to companies or entities in the EU that collect, store, or process personal data, as well as to organizations outside the EU that handle the personal data of EU residents.

GDPR is designed to reinforce protections around personal information and unify requirements on businesses and agencies throughout the EU.

> Overall, the goal of GDPR is to provide European residents with transparency of how their PII [Personally Identifiable Information] data is used, improve the level of control over their own data and increase the safeguards used to protect that data.[1]

A Broader Definition of PII

Under GDPR, PII is defined as any piece of information relating to an identified or identifiable person.[2] Beyond an individual's name, social security number, and date of birth details, this broader definition includes biometric (finger prints, facial recognition, body measurements), ethnic, demographic, political, religious, location, health, and genetic information, as well as IP address and web browser history including cookies. The regulations are applicable to all personal information that an organization currently holds, regardless of when the data was collected.

To protect individuals, GDPR requires clear language in privacy policies, user consent, and greater transparency on the transfer and use of PII, and holds organizations accountable for how they handle it. And the stakes are high: GDPR includes steep financial penalties for failing to comply.

Overview of GDPR

GDPR can be briefly summarized in rules for organizations and rights for citizens:

---

[1] Kawamoto, Dawn. "Will GDPR Rules Impact States and Localities?" *State & Local Government News Articles*, Government Technology, 3 May 2018.

[2] Article 4(1) of the General Data Protection Regulation states that "…an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person…"

Rules for Organizations	Rights for Citizens
Accountability The responsibility to secure the data organizations hold, maintain records of data processing activities, and only permit data transfers to other organizations if appropriate protections are in place. **Data Protection Impact Assessment** For major projects impacting personal data, large corporations and EU agencies must conduct an assessment to help identify and minimize risks to data. If the US adopted similar measures, courts would be included in this requirement. **Data Protection Officer** Public authorities (including courts) in the EU are required to appoint a Data Protection Officer whose job it is to ensure that both processes and technology keep personal data secure. Data protection requirements also extend to external vendors; contracts or other legal guarantees are required to ensure that vendors meet GDPR security standards. **Data Breach Reporting** If personal data is deleted, disclosed accidentally or unlawfully to unauthorized recipients, or is temporarily unavailable or altered, organizations must notify the EU's Data Protection Authority (DPA) within 72 hours of becoming aware of the breach. Public entities may also be required to inform individuals about the breach. **Contesting Automated Decisions** When algorithms are being used to make decisions, organizations must provide a process for contesting and/or opting out of those processes.	**Transparency** Data policies must be transparent to an average person. Key information can't be buried in lengthy legalese jargon. **Consent** People must give explicit consent for most kinds of data collection, and they must be able to easily withdraw that consent. **Access and Rectification** A person's right to see data that concerns them and the right to have inaccuracies corrected. Individuals cannot be charged for access to their data, and organizations are required to correct inaccuracies quickly - generally within one month. **Erasure – aka the Right to be "Forgotten"** With some exceptions, organizations must delete data that is no longer needed, or data that was collected when someone was a child, if an individual requests it. Organizations must also take steps to request the data also be deleted by other entities with whom the data was shared. **Object** The right to object to the use of personal data and stop it from being used, even if it is being used for legitimate, lawful "public" tasks. Data used for the "establishment, exercise or defense of legal claims"[3] (court data) is exempt from such objections. **Data Portability** The right to move personal data from one service provider to another. **Automated Processing** The right not to be subjected to an automated decision.

[3] "Right to Object." *ICO*, United Kingdom Information Communications Office, accessed 3 August 2018.

While individual protections are at the core of GDPR, there are also important common-sense limitations: organizations can collect personal information without consent if the entity's "legitimate interests" outweigh a person's rights and freedoms.[4] "Legitimate interests" include fraud prevention, internal administration, information security, and reporting possible criminal acts.

Potential Impacts on US Litigation

GDPR only applies to data collected or processed in the EU. It does not apply to all data collected and processed about residents or citizens of the EU.

> GDPR does not apply if a U.S. government agency collects PII data on a citizen of Europe who is visiting or living in the U.S. and uses that government agency's services or products while in the U.S…[5]

Since US courts do not collect or process data in the EU, the legislation has little direct impact. In fairly rare instances, US courts may collect, store, or process litigant data that has a European nexus.

One potential that is not yet well understood is how GDPR might impact discovery in multi-national litigation. While a litigant in the US may ask for information that includes personal data of an EU subject, the European entity holding the data may be restricted from providing it. US discovery rules may call for disclosure, while GDPR may specify that the organization not disclose the information or may require that the information be shared but limit the mechanisms that can be used to transfer the data.

Considerations for US Courts

Data privacy law is dynamic, changing, and become more stringent. This trend is likely to continue. GDPR is a "sea-change" in privacy law. The clearest indication of GDPR's potential impact on US courts is the speed with which California crafted and passed similar privacy legislation.[6] Where California goes, the rest of the US seems destined to follow.

More than 15 years ago, California lead the nation by enacting the first data breach statute. Alabama and South Dakota were the last, with their laws taking effect mid-2018. Even though all 50 states now have some kind of data breach notification requirements, each state has its own definition of personal information and what constitutes a data breach. Requirements for responding vary widely, as do penalties for failing to comply. Most states do not protect personal information contained in paper records.

---

[4] "The EU General Data Protection Regulation – Questions and Answers." *Human Rights Watch*, 6 June 2018.

[5] Kawamoto, Dawn. "Will GDPR Rules Impact States and Localities?" *Government Technology: State & Local Government News Articles*, Government Technology, 3 May 2018,

[6] Kirk, Jeremy. "California's New Privacy Law: It's Almost GDPR in the US." *Bank Information Security*, Information Security Media Group, 2 July 2018

Understanding and complying with the unique complexities of privacy law across different jurisdictions is a burden on business. Unifying data privacy regulations has decomplicated doing business across the EU. Now there are signs that European organizations view US data protection as inadequate, putting US companies at a competitive disadvantage. Overnight, it seems, GDPR-compliance has become "best practice" expectation.

EU data privacy regulations are influencing policies and practices as well as consumer expectations globally. If California's Consumer Privacy Act is an indicator, it will be only a matter of months before other US states enact similar protections.[7] However, privacy legislation at the state level would create a patchwork of unique regulations that would be both a compliance burden and an enforcement challenge. While there are sure to be legal challenges to California's legislation before it goes into effect in 2020, US consumers aren't likely to accept the status quo. In Europe, consumer advocates – bolstered by the publicity surrounding a couple of very notable data breaches – ultimately won out over well-funded business interests aligned against the legislation[8].

If EU data privacy standards were applied to US courts, the sensitive nature of court data would warrant the most stringent protections. The EU's legislation is a call-to-action and US courts should have at least a basic understanding of the legislation and a game plan for preparing to comply with similar legislation in the US.

[7] Slefo, George P. "Marketers and Tech Companies Confront California's Version of GDPR." *Ad Age*, 29 June 2018

[8] Kalyanpur, Nikhil, and Abraham Newman. "Analysis | Today, a New E.U. Law Transforms Privacy Rights for Everyone. Without Edward Snowden, It Might Never Have Happened." *The Washington Post*, WP Company, 25 May 2018.