RAPP

Global Data Protection and Privacy Legislation

2018 Pocket Guide

Table of Contents

Introduction

THE DAWN OF A NEW DAY IN DATA PROTECTION

Data-protection laws are rapidly changing to give consumers more control over their personal information and how it's used in commerce. These regulations represent a seismic shift in electronic communications across the marketing industry — a shift away from connectivity based on opt-out strategies to new standards that require marketers to obtain opt-in consent before initiating contact.

The path has been forged by the European Commission and a new set of data-protection laws that went into effect on April 14, 2016, covering all countries in the European Union.[1] These EU regulations are among the world's most stringent and are quickly becoming the new standard against which other countries measure their own laws.

The U.S., on the other hand, lacks significant legislation and instead has laws that vary by industry. But with Canada, Latin America and several parts of Asia keeping pace with EU laws, most people believe it's just a matter of time before the U.S. adopts more universal laws governing data protection and privacy.

WHY DOES THIS MATTER TO YOU?

Legislation isn't necessarily bad news for marketers. By increasing the stakes for protecting personal information, these laws signify the beginning of a new social contract between marketers and consumers. Ultimately, this makes brands less reliant on third-party data held within the walled gardens of Facebook, Google and other large technology firms, and more reliant on their own first-party data. This is especially relevant as consumers increasingly voice concerns about trusting small and large enterprises — and for that matter, national and global corporations — with their personal data.

As new data-protection laws are being enacted across the globe, many organizations are struggling to update international business strategies, practices and processes amidst confusion around data sovereignty. Confusion abounds, with laws, regulations and penalties varying greatly from region to region and country to country.

1. "Joint Statement on the Final Adoption of the New EU Rules for Personal Data Protection," Brussels, April 14, 2016.

In a digital-smart, mobile world, ignoring global cross-nationalization of data etiquette and data protection is to fundamentally disregard the worldwide demand for the basic on- and off-line rights of every consumer, customer and prospect. These shifts are ones we simply cannot ignore.

Open freedoms or weak data laws in some major countries should not be used as a forgiveness note for bad brand behavior. It's important to act with courtesy and sensibility by always keeping data etiquette, user sensibility and security compliance in mind.

ABOUT THIS POCKET GUIDE

Within this pocket guide, we provide a snapshot of global privacy laws and explore legislation in key regions, namely the EU and the U.S. As brands and businesses continue to grow, pushing the boundaries of what's possible technologically to build and strengthen long-lasting, valued relationships with consumers, there is an ever-growing demand for clarity and fluency. We hope this pocket guide goes some way in helping you to navigate the data-protection sphere.

The legislative landscape is constantly evolving, and we encourage you to consult counsel before making any legal decisions based on this information. We continue to monitor the legislative landscape and will update this pocket guide as laws and regulations evolve.

ABOUT RAPP'S CONSUMER TRUST COUNCIL

The Consumer Trust Council is a global network of cross-disciplinary RAPP leaders dedicated to the advancement of data-driven marketing practices in accordance with evolving privacy legislation, data ethics and consumer trust standards. Our mission is to lead the agency and the industry toward more mindful, privacy-conscious marketing designed for the opt-in world. The Council is comprised of experts across technology, data, analytics, media, strategy and experience design who maintain active certifications and credentials from institutions including the IAPP, ISACA, British Computer Society and PACE.

Methodology

LEGISLATING THE PERSONAL DATA REVOLUTION

The trend is being led by the European Commission and a new set of data-protection laws that went into effect on April 14, 2016, covering all countries in the European Union. The EU's new privacy "bill of rights" ensures that consumers have easier access to their own data and provides the right to data portability between service providers, the "right to erasure" and the right to know when personal data has been hacked.

According to a recent Eurobarometer survey, 67% of Europeans said they are concerned about not having complete control over the information they provide online, and 70% said they worry about what companies will do with the information they disclose.[2] In adopting these new laws, the EU sends a clear message that people have a fundamental right to control their personal data.

COUNTRY ASSESSMENT/SELECTION

The countries listed in this report were selected, among other things, using Forrester's 2015 Data Privacy Heat Map. The nine key provisions outlined in this report reflect the fundamental pillars of the EU General Data Protection Regulation (GDPR): Opt-In/Consent, Right to Erasure, Data Transfer, Disclosure, Enforcement, Accountability–Privacy By Design, Breach Notification, Access and Opt-Out.

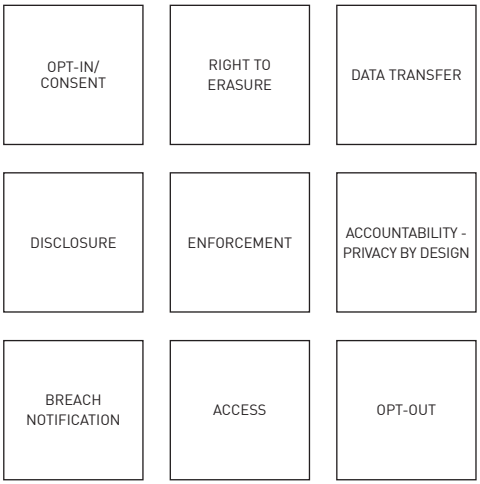
Each of the nine key provisions was factored in the assessment of the overall data privacy and protection legislative framework of each country. Adoption and compliance strength of these provisions was qualitatively assessed using DLA Piper's Data Protection Laws of the World Handbook.

2. "Agreement on Commission's EU Data Protection Reform will Boost Digital Single Market," Brussels, December 15, 2015.

BENCHMARKING DATA PROTECTION/PRIVACY LEGISLATION AGAINST THE GENERAL DATA PROTECTION REGULATION

In this pocket guide, we have taken the nine key provisions of the EU GDPR and assessed the adoption and strength of these from 51 countries around the world. Understanding the global data privacy/protection legislative landscape is key to ensuring compliance and brand awareness.

Every country selected in this pocket guide follows the same assessment format. A three-by-three chart is used to map out the nine key provisions of the GDPR and then color-coded based on adoption and compliance strength.



RED – A red square represents little to no legislation in the labeled key provision. Red is indicative of weak EU standards.

YELLOW – A yellow square represents some legislation in the labeled key provision. Yellow is indicative of "loose adoption" of EU standards.

GREEN – A green square represents strong legislation in the labeled key provision. Green is indicative of strong EU standards.

Methodology Continued

OPT-IN/CONSENT

EXPLICIT CONSENT

Express or direct consent means that an individual is clearly presented with an option to agree or disagree with the collection, use or disclosure of personal information. Explicit consent is usually required when clear, documentable consent is required, and the purposes for which it is being provided are sensitive. Explicit consent can be provided verbally or in writing.

IMPLICIT CONSENT

Indirect consent can mean two things:

1. You volunteer personal information for an organization to collect, use or disclose for purposes that would be considered obvious at the time.
2. You provide personal information to an organization, and it is used in a way that clearly benefits you and the organization's expectations are reasonable. Implied consent is usually inferred from your actions and the current circumstance you are in.[3]

RIGHT TO ERASURE

"Right to Erasure" legislation grants data subjects the right to obtain from the controller the erasure of personal data relating to them.

BREACH NOTIFICATION

Countries with "Breach Notification" laws typically have provisions regarding who must comply with the laws (e.g., businesses, data/information brokers, government entities, etc.), definitions of "personal information," what constitutes a breach and requirements for notice (e.g., timing or method of notice, who must be notified).

3. "Different Types of Consent," PrivacySense.net, 2015.

DATA TRANSFER

"Data Transfer" legislation ensures that data controllers and processors take special precautions when transferring personal data to other countries, ensuring adequate data protection standards in those countries.

DISCLOSURE

Subjects whose personal data is being collected are informed as to the party or parties collecting that data and the purpose for which the data is being collected.

ACCOUNTABILITY–PRIVACY BY DESIGN

Data controllers and processors comply with "Privacy by Design" legislation if they take reasonable technical and organizational measures to ensure the security and confidentiality of a subject's personal data.

ENFORCEMENT

Compliance with data-protection laws is generally enforced through fines, criminal liability, civil liability and injunctive reliefs.

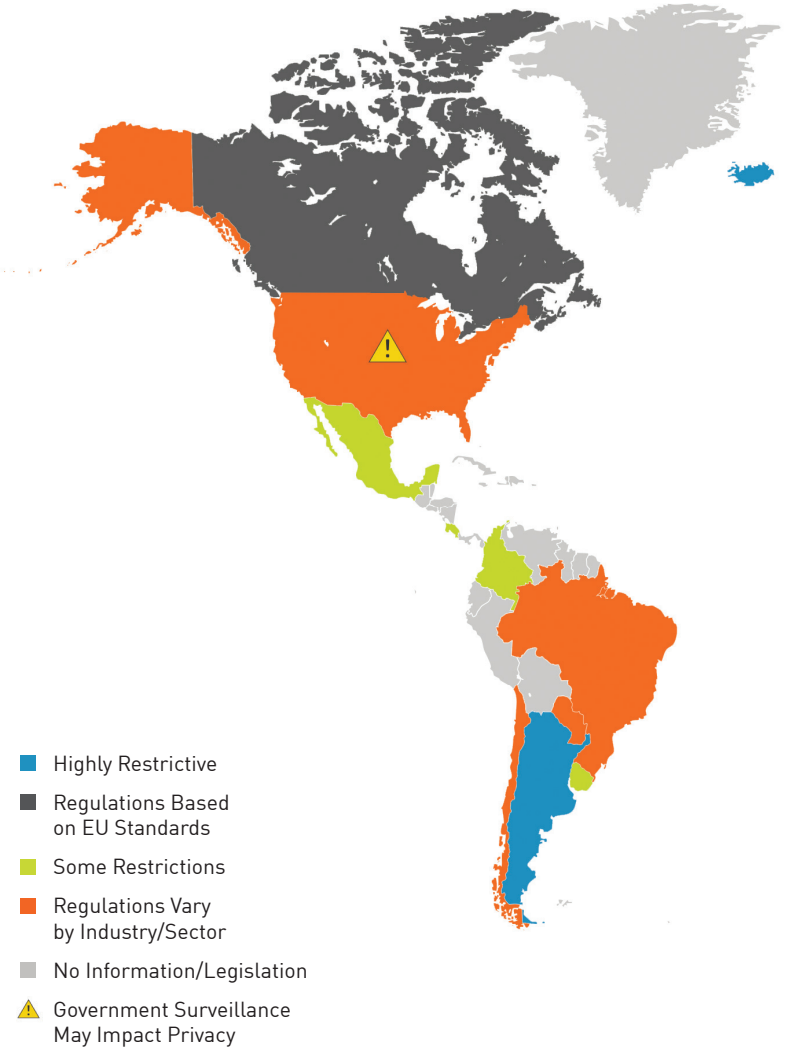
ACCESS

Gives data subjects the right to access their personal data and correct any inaccuracies.

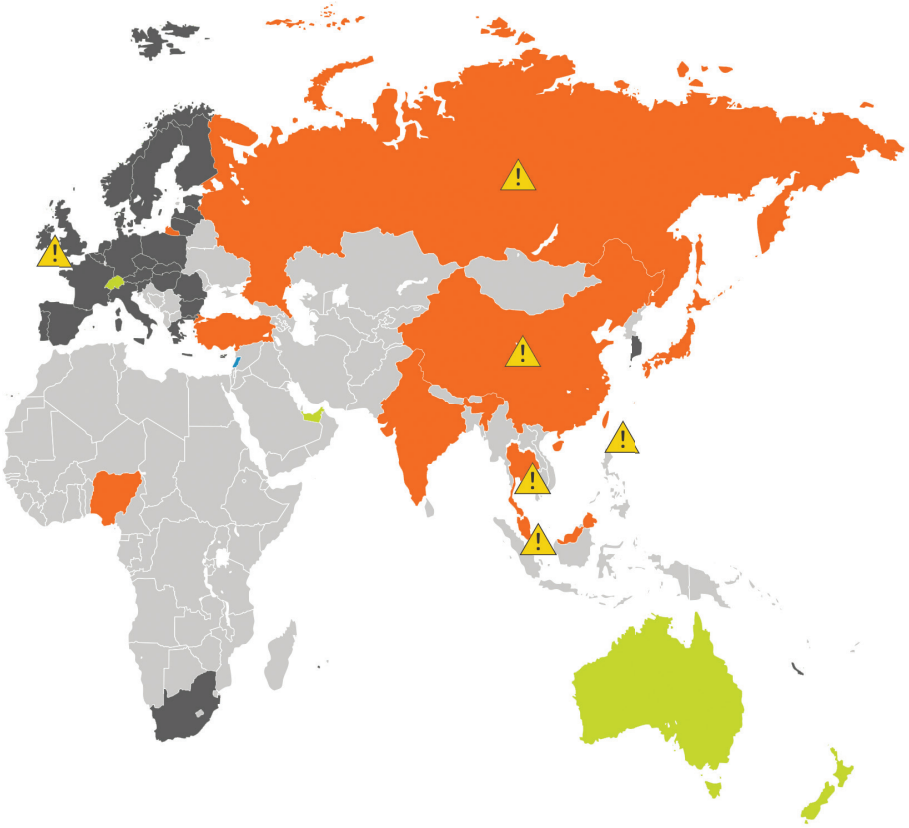
OPT-OUT

"Opt-Out" legislation ensures data controllers have an opt-out mechanism in place to allow data subjects to withdraw consent at any time.

2015 Global Data Privacy Heat Map[4]



4. Forrester's 2015 Data Privacy Heat Map, Forrester Research, Inc, published October 2015.




Departures

Privacy and Data Protection by Country

European Union

The EU General Data Protection Regulation (GDPR) unifies data-protection laws across the EU with a single set of rules that replaces the existing 1995 Data Protection Directive. The GDPR aims to modernize existing privacy laws to meet the challenges of new technologies, strengthen individuals' rights while promoting the free flow of personal data throughout the EU and achieve consistent implementation of data-protection policies in all EU Member States.

Under the new GDPR, fines increase up to €20 million per violation, or 4% of global annual turnover. Though the GDPR went into effect on April 14, 2016, the new penalties will not be levied until 2018, following a two-year grace period to provide companies sufficient time to comply.

On December 17, 2015, after three years of drafting and negotiations, the European Parliament and Council of the European Union reached an informal agreement on the final draft of the EU General Data Protection Regulation. The stated objective of the GDPR is twofold: (1) to enhance data-protection rights of individuals; and (2) to improve business opportunities by facilitating the free flow of personal data in the digital single market; treating 28 national markets as one united entity. Important differences between the 1995 law and pending GDPR legislation are noted below.

CONSENT

A key provision of the new law deals with consent, and the fact that "implied" consent is no longer a legal basis, thus significantly increasing the importance of opt-in for brand/consumer relationships. Consent for children under 13 must be given by a parent or custodian and should be verifiable.

The GDPR states that in order for personal data to be processed by a controller or processor, they must have proof of freely given, valid, informed and explicit/unambiguous consent. "To meet the consent category under the GDPR, the data controller must obtain written, explicit consent for the specified purpose. Implied consent is no longer a legal basis. Consent is not valid where there is an imbalance between the data subject and the controller, and the data subject has the right to withdraw consent at any time."[5]

5. Harvard's Journal of Law & Public Policy: Updating the Law of Information Privacy — the New Framework of the European Union.

THE DATA PROTECTION OFFICER

The GDPR will require global companies to appoint an independent Data Protection Officer (DPO) to comply with tougher regulations on data protection across all 28 EU Member States. DPOs must be independent and have their own support teams.

ACCOUNTABILITY–PRIVACY BY DESIGN

Another new provision of the GDPR extends its reach to products and systems not yet developed, ensuring that business innovation is always grounded in data protections for the consumer. Data protection must be built into business processes and systems from the start and provided by default. Whenever a business develops or designs a new technology, product or service, it should do so in a way that ensures compliance with data-protection obligations.[6]

THE RIGHT TO ERASURE

The "right to be forgotten" was replaced by a more limited "right to erasure" in the version of the GDPR adopted by the European Parliament in March 2014. Article 17 provides that the data subject has the right to request erasure of personal data on any one of a number of grounds, but primarily in cases where the legitimate interests of the company are overridden by the interests or fundamental rights and freedoms of the individual.[7]

MANDATORY BREACH NOTIFICATION

Any breaches of personal data must be reported to authorities and affected individuals. This must be done with undue delay, and where feasible, within 72 hours of awareness. (Notification isn't required if a breach is unlikely to pose a risk to the rights and freedoms of individuals.) Regardless, all companies must adopt internal procedures for handling data breaches.

PENALTIES FOR NON-COMPLIANCE

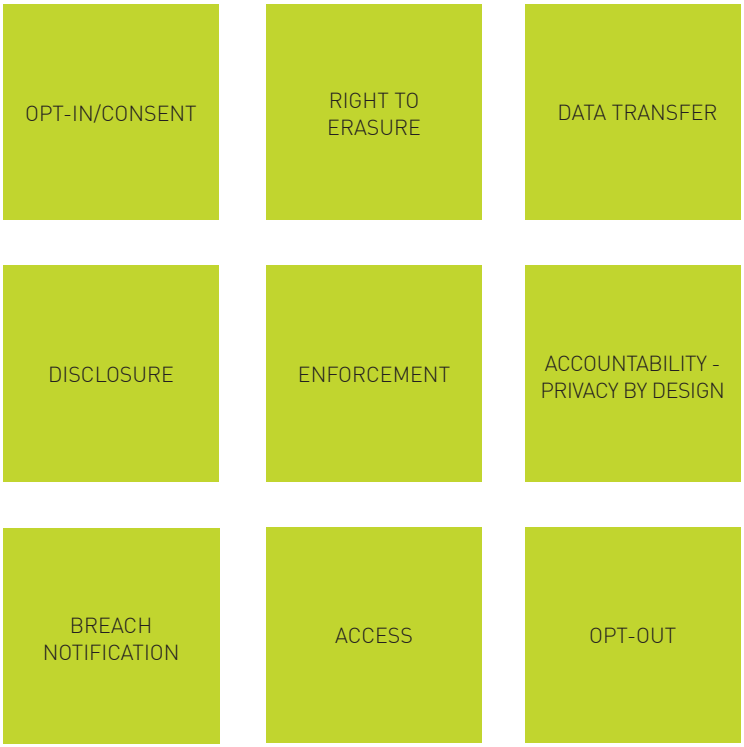
The most serious breaches of the GDPR could result in fines of up to €20 million, or 4% of global annual turnover, whichever is higher. These new penalties will be enforced after two years to provide companies with time to make operations compliant.

6. Hunton and Williams, LLC, Guide to the EU General Data Protection Regulation, July 2015.
7. "The Right to Be Forgotten," Pupil Barrister and Oliver Hyams, May 2014.

European Union Continued

EU DEFINITION OF PERSONAL DATA

According to the EU Commission, personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a photo, an email address, bank details, medical information, computer IP address or any factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity. The EU Charter of Fundamental Rights says that everyone has the right to personal data protection in all aspects of life: at home, at work, while shopping, while receiving medical treatment, at a police station or on the Internet.[8]



8. From the European Commission's Press Release Announcing the Proposed Comprehensive Reform of Data Protection Rules, January 25, 2012.

United States

CURRENT LEGISLATION: A PATCHWORK QUILT

HIPAA	COPPA	GLBA	PHI	ePHI	CAN-SPAM	TCPA	HITECH	JFPA

The U.S. does not have universal data-protection/privacy legislation, but rather a collection of laws that govern data privacy at the industry level. And unlike the more stringent EU data-protection laws, U.S. law generally requires a pre-collection notice and an opt-out option — rather than an opt-in option — for the use and disclosure of regulated personal information. One notable exception to the lack of universal federal law in the U.S. is the Children's Online Privacy Protection Act of 1998 (COPPA), which governs the online collection of information from children under the age of 13.[9]

Recently, the U.S. Department of Commerce and the European Commission introduced the EU-U.S. Privacy Shield, a legislative framework designed to replace the previously invalidated Safe Harbor framework. The EU-U.S. Privacy Shield provides a mechanism for U.S. companies to comply with EU data-protection laws when transferring personal data from the European Union to the United States. Commitment to the EU-U.S. Privacy Shield is enforcible under U.S. law.

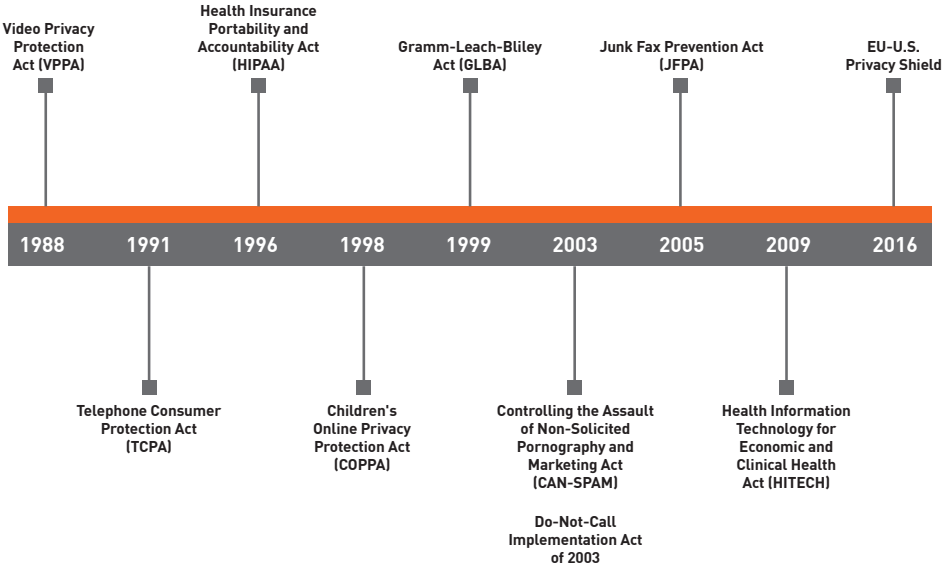
There are many sources of privacy law in the U.S. at both the federal and state levels. These laws and regulations may be enforced by federal and state authorities, and many provide individuals with a private right to bring lawsuits against organizations they believe are violating the law.

The primary industries that are regulated under U.S. data-privacy law are healthcare and financial services. In financial services, various regulators, including state insurance regulators, have adopted standards under the Gramm-Leach-Bliley Act (GLBA) that dictate how companies collect, use and disclose non-public personal information. In healthcare, the Department of Health and Human Services (HHS) is responsible for enforcement of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Outside of regulated industries, the Federal Trade Commission (FTC) and the Federal Communications Commission (FCC) are the primary federal privacy regulators in the U.S.

9. US FTC Complying With COPPA: Frequently Asked Questions.

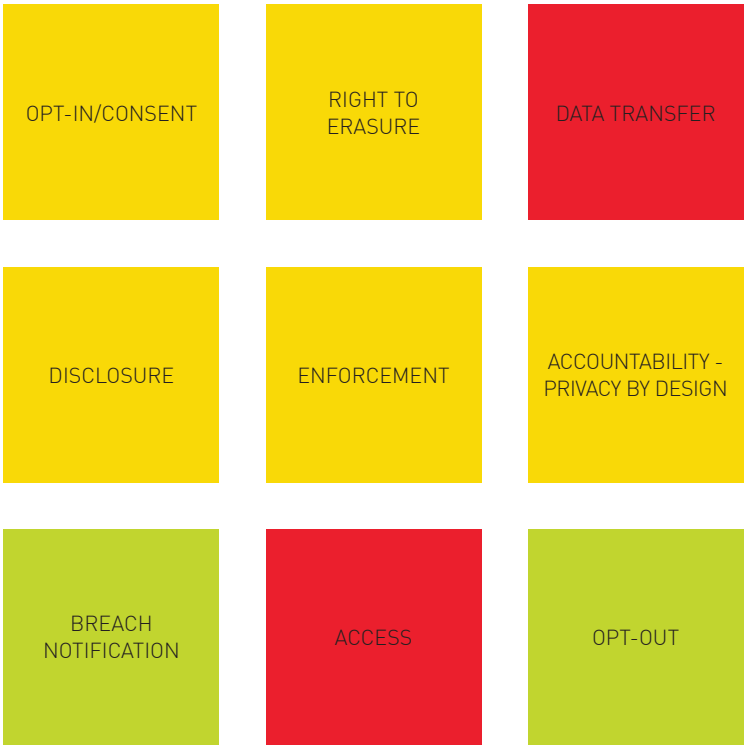
United States Continued

What's remarkable about the history of data-protection laws in the U.S. is the absence of significant legislation over the past 10 years, despite the proliferation of consumer data and increasing concerns regarding data privacy, abuse and theft. The last major piece of legislation, from 2005, governed the use of the fax machine by marketers (the Junk Fax Prevention Act [JFPA]); the HITECH Act of 2009 simply increased the penalties for HIPAA violations, and the EU-U.S. Privacy Shield protects EU citizens only.



DEFINITION OF PERSONAL DATA

The U.S. defines personally identifiable information (PII) as any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, computer IP address, date and place of birth, mother's maiden name or biometric records (including photos, X-rays, fingerprints or other biometric data); and (2) any other information that is linked or linkable to an individual in conjunction with other data, such as race, religion, weight, activities, geographical indicators and employment/medical/educational/financial data.[10] Generally speaking, enforcement of privacy laws in the U.S. are subject to the definition of PII.



10. NIST – US Department of Commerce: Guide to Protecting the Confidentiality of PPI, SP 800-122.

Argentina

The Argentine Data Protection Regulation (ADPR) addresses the treatment and processing of personal data. Article 43 of the Argentinian national constitution gives any person the right to gain access to information about them contained in public and private databases. It also grants them the right to demand incomplete or partially false data to be amended or suppressed. In 2015, Argentina also passed new data-privacy regulations pertaining to the use of CCTV as well as more clearly defined DPA sanctions for data-privacy violations related to the use of "do not call" registries.

OPT-IN/CONSENT	RIGHT TO ERASURE	DATA TRANSFER
DISCLOSURE	ENFORCEMENT	ACCOUNTABILITY - PRIVACY BY DESIGN
BREACH NOTIFICATION	ACCESS	OPT-OUT

Australia

In Australia, the federal Privacy Act 1988 regulates the collection, use and disclosure of personal data. In March 2014, significant amendments to the Privacy Act were made with the introduction of the Australian Privacy Principles (APPs). The APPs strengthen direct marketing and cross-border transfer provisions as well as security, access and correction of personal information.

Austria

The EU General Data Protection Regulation (GDPR) is a proposal that will unify data-protection laws across the EU with a single set of rules that replaces the existing 1995 Data Protection Directive. The GDPR aims to modernize existing privacy laws to meet the challenges of new technologies, strengthen individuals' rights while promoting the free flow of personal data throughout the EU and achieve consistent implementation of data-protection policies in all EU Member States, including Austria.

OPT-IN/CONSENT	RIGHT TO ERASURE	DATA TRANSFER
DISCLOSURE	ENFORCEMENT	ACCOUNTABILITY - PRIVACY BY DESIGN
BREACH NOTIFICATION	ACCESS	OPT-OUT

Belgium

The EU General Data Protection Regulation (GDPR) is a proposal that will unify data-protection laws across the EU with a single set of rules that replaces the existing 1995 Data Protection Directive. The GDPR aims to modernize existing privacy laws to meet the challenges of new technologies, strengthen individuals' rights while promoting the free flow of personal data throughout the EU and achieve consistent implementation of data-protection policies in all EU Member States, including Belgium.

Brazil

The Brazilian Civil Rights Framework for the Internet (*Marco Civil Da Internet*), enacted on April 23, 2014, establishes a number of rights for Internet users in Brazil and addresses concerns regarding the collection, maintenance, treatment and use of personal data on the Internet. The Brazilian Internet Act applies to ISPs (Internet Service Providers) and IAPs (Internet Application Providers). Some of the key provisions address issues related to freedom of expression, interoperability, the use of open standards and technology, intermediary liability, net neutrality, privacy, accessibility, open government data and data retention. Although there are no restrictions on data transfers outside of Brazil, foreign companies who store Brazilian personal data must comply with the Brazilian laws.

Bulgaria

The EU General Data Protection Regulation (GDPR) is a proposal that will unify data-protection laws across the EU with a single set of rules that replaces the existing 1995 Data Protection Directive. The GDPR aims to modernize existing privacy laws to meet the challenges of new technologies, strengthen individuals' rights while promoting the free flow of personal data throughout the EU and achieve consistent implementation of data-protection policies in all EU Member States, including Bulgaria.

OPT-IN/CONSENT	RIGHT TO ERASURE	DATA TRANSFER
DISCLOSURE	ENFORCEMENT	ACCOUNTABILITY - PRIVACY BY DESIGN
BREACH NOTIFICATION	ACCESS	OPT-OUT

Canada

Canadian law requires businesses to obtain expressed or implied opt-in consent before any commercial electronic contact with a customer is initiated. Canada's Anti-Spam Legislation (CASL), effective as of July 1, 2014, covers email like the U.S. CAN-SPAM Act, but also addresses social networking accounts and text messages sent to a cell phone. New rules effective in January 2015 made it illegal to install programs (malware) on someone's computer without consent. Organizations that don't comply with CASL risk serious penalties, including criminal charges, civil charges, personal liability for company officers and directors and penalties of up to $10 million.

Chile

Chile's Personal Data Protection Law (PDPL) regulates the treatment of personal information in public and private databases. The PDPL generally requires organizations to obtain consent from data subjects before processing their personal data. The transfer of personal data to other countries is considered a form of processing and therefore must meet the consent requirements established by the PDPL.

China

China's data-protection and privacy legislation is influenced by the EU Data Protection Directive. The Chinese government has made an effort recently to move the country towards a more comprehensive data-privacy regime. However, similar to U.S. law, the totality of the regulations governing the use of personal data fall under a number of different sectoral and regional laws. Under current law, an operator may not send a consumer commercial information unless on the request or with the consent of the consumer. An October 2013 amendment to the Consumer Rights Law extended protections to include a "junk-information" nuisance provision.

Costa Rica

Data regulation in Costa Rica consists of two pieces of legislation: the Undisclosed Information Law and the Protection in the Handling of the Personal Data of Individuals. Organizations must obtain express and valid consent before processing personal data. Individuals have the right to dispute any erroneous or misleading information about them. Costa Rica does not have mandatory breach notification requirements.

Cyprus

The EU General Data Protection Regulation (GDPR) is a proposal that will unify data-protection laws across the EU with a single set of rules that replaces the existing 1995 Data Protection Directive. The GDPR aims to modernize existing privacy laws to meet the challenges of new technologies, strengthen individuals' rights while promoting the free flow of personal data throughout the EU and achieve consistent implementation of data-protection policies in all EU Member States, including Cyprus.

Czech Republic

The EU General Data Protection Regulation (GDPR) is a proposal that will unify data-protection laws across the EU with a single set of rules that replaces the existing 1995 Data Protection Directive. The GDPR aims to modernize existing privacy laws to meet the challenges of new technologies, strengthen individuals' rights while promoting the free flow of personal data throughout the EU and achieve consistent implementation of data-protection policies in all EU Member States, including the Czech Republic.

Denmark

The EU General Data Protection Regulation (GDPR) is a proposal that will unify data-protection laws across the EU with a single set of rules that replaces the existing 1995 Data Protection Directive. The GDPR aims to modernize existing privacy laws to meet the challenges of new technologies, strengthen individuals' rights while promoting the free flow of personal data throughout the EU and achieve consistent implementation of data-protection policies in all EU Member States, including Denmark.

UAE – Dubai

There is no dedicated data-protection law or national data-protection regulator in the United Arab Emirates (UAE). And like the U.S., regulation of data processing varies by industry, with healthcare and financial services as the two primary regulated industries. There are several independent jurisdictions, also known as "free zones," with their own legal systems and courts separate from those in the wider UAE (DIFC and DHCC). These free zones have jurisdiction over corporate, commercial, civil, employment, trusts and securities law matters. They have data-protection laws that model the EU Data Protection Directive.

Finland

The EU General Data Protection Regulation (GDPR) is a proposal that will unify data-protection laws across the EU with a single set of rules that replaces the existing 1995 Data Protection Directive. The GDPR aims to modernize existing privacy laws to meet the challenges of new technologies, strengthen individuals' rights while promoting the free flow of personal data throughout the EU and achieve consistent implementation of data-protection policies in all EU Member States, including Finland.

France

The EU General Data Protection Regulation (GDPR) is a proposal that will unify data-protection laws across the EU with a single set of rules that replaces the existing 1995 Data Protection Directive. The GDPR aims to modernize existing privacy laws to meet the challenges of new technologies, strengthen individuals' rights while promoting the free flow of personal data throughout the EU and achieve consistent implementation of data-protection policies in all EU Member States, including France.

Germany

The EU General Data Protection Regulation (GDPR) is a proposal that will unify data-protection laws across the EU with a single set of rules that replaces the existing 1995 Data Protection Directive. The GDPR aims to modernize existing privacy laws to meet the challenges of new technologies, strengthen individuals' rights while promoting the free flow of personal data throughout the EU and achieve consistent implementation of data-protection policies in all EU Member States, including Germany.

Greece

The EU General Data Protection Regulation (GDPR) is a proposal that will unify data-protection laws across the EU with a single set of rules that replaces the existing 1995 Data Protection Directive. The GDPR aims to modernize existing privacy laws to meet the challenges of new technologies, strengthen individuals' rights while promoting the free flow of personal data throughout the EU and achieve consistent implementation of data-protection policies in all EU Member States, including Greece.

Hong Kong

Hong Kong's Personal Data Privacy Ordinance (PDPO) regulates the collection and processing of personal data. Organizations who collect data must inform data subjects of the purpose for which the data is being used, the person to whom the data may be transferred to and the data subject's right to request access and/or correction of their personal data. Currently, there is no mandatory legal requirement under the ordinance for data users to notify authorities or data subjects about data breaches in Hong Kong.

Hungary

The EU General Data Protection Regulation (GDPR) is a proposal that will unify data-protection laws across the EU with a single set of rules that replaces the existing 1995 Data Protection Directive. The GDPR aims to modernize existing privacy laws to meet the challenges of new technologies, strengthen individuals' rights while promoting the free flow of personal data throughout the EU and achieve consistent implementation of data-protection policies in all EU Member States, including Hungary.

Iceland

Data protection in Iceland is regulated by Act 77/2000 on the Protection and Processing of Personal Data (Data Protection Act), which mirrors the EU Data Protection Directive. Data processors may only collect and process personal data if the data subject has given consent. The transfer of personal data to other countries is prohibited if those countries do no provide an adequate level of personal data protection. Data processors may only transfer personal data if the data subject has consented to the transfer. Iceland does not have breach notification requirements.

India

Data-protection legislation in India is somewhat fragmented, mainly consisting of the Information Technology Act, 2000 (the Act) and the Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules (Privacy Rules). Under the Privacy Rules, organizations must obtain consent from data subjects before processing their personal data. The Privacy Rules also mandate that data subjects be informed of an organization's practices regarding the handling and disclosure of personal information. India has strong breach notification requirements under the Information Technology Rules, 2013 (Cert-In Rules).

Ireland

The EU General Data Protection Regulation (GDPR) is a proposal that will unify data-protection laws across the EU with a single set of rules that replaces the existing 1995 Data Protection Directive. The GDPR aims to modernize existing privacy laws to meet the challenges of new technologies, strengthen individuals' rights while promoting the free flow of personal data throughout the EU and achieve consistent implementation of data-protection policies in all EU Member States, including Ireland.

Israel

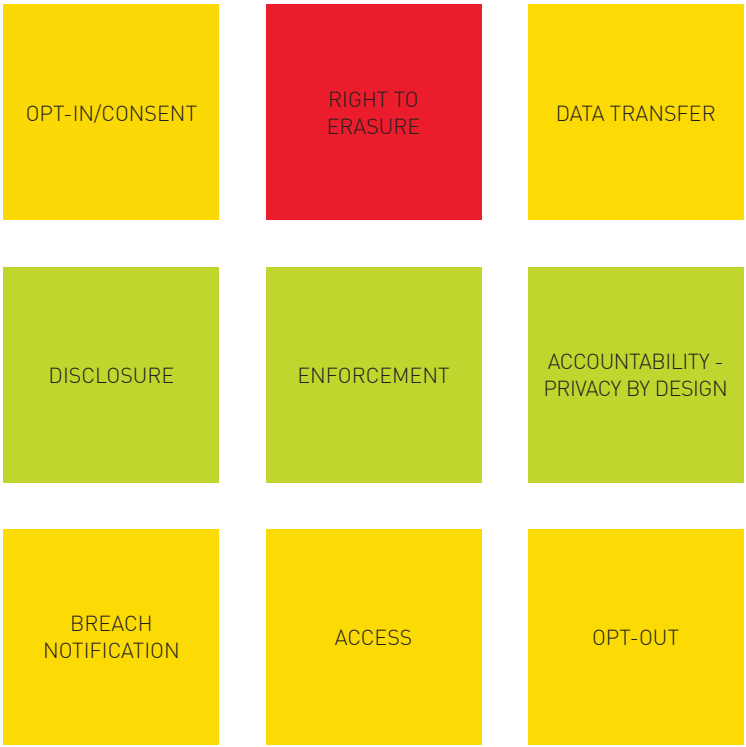
Both the Protection of Privacy Law, 5741-1981 (PPL) and the Basic Law: Human Dignity and Liberty, 5752-1992 govern the right to privacy in Israel. Data processors must obtain informed consent from data subjects before processing their personal data. Transfer of personal data to other countries is only allowed if those countries ensure a level of personal data protection equivalent to Israel.

Italy

The EU General Data Protection Regulation (GDPR) is a proposal that will unify data-protection laws across the EU with a single set of rules that replaces the existing 1995 Data Protection Directive. The GDPR aims to modernize existing privacy laws to meet the challenges of new technologies, strengthen individuals' rights while promoting the free flow of personal data throughout the EU and achieve consistent implementation of data-protection policies in all EU Member States, including Italy.

Japan

Data-protection legislation in Japan is mainly regulated by the Act on the Protection of Personal Information (APPI). Under the APPI, data processors must specify the purpose of use of personal information being collected before processing it. Organizations must also obtain consent from data subjects if they want to use personal information beyond the initial communicated purpose of use.



Latvia

The EU General Data Protection Regulation (GDPR) is a proposal that will unify data-protection laws across the EU with a single set of rules that replaces the existing 1995 Data Protection Directive. The GDPR aims to modernize existing privacy laws to meet the challenges of new technologies, strengthen individuals' rights while promoting the free flow of personal data throughout the EU and achieve consistent implementation of data-protection policies in all EU Member States, including Latvia.

Lithuania

The EU General Data Protection Regulation (GDPR) is a proposal that will unify data-protection laws across the EU with a single set of rules that replaces the existing 1995 Data Protection Directive. The GDPR aims to modernize existing privacy laws to meet the challenges of new technologies, strengthen individuals' rights while promoting the free flow of personal data throughout the EU and achieve consistent implementation of data-protection policies in all EU Member States, including Lithuania.

Luxembourg

The EU General Data Protection Regulation (GDPR) is a proposal that will unify data-protection laws across the EU with a single set of rules that replaces the existing 1995 Data Protection Directive. The GDPR aims to modernize existing privacy laws to meet the challenges of new technologies, strengthen individuals' rights while promoting the free flow of personal data throughout the EU and achieve consistent implementation of data-protection policies in all EU Member States, including Luxembourg.

OPT-IN/CONSENT	RIGHT TO ERASURE	DATA TRANSFER
DISCLOSURE	ENFORCEMENT	ACCOUNTABILITY - PRIVACY BY DESIGN
BREACH NOTIFICATION	ACCESS	OPT-OUT

Malaysia

Malaysia passed the Personal Data Protection Act (PDPA) on June 2, 2010. Under the PDPA, data processors are required to obtain consent from data subjects before processing their personal information. Data processors must also inform data subjects of the purpose for which their personal data is being collected. There are no provisions in the PDPA that address breach notification requirements.

Mexico

Mexico enacted the Federal Law on the Protection of Personal Data held by Private Parties on July 5, 2010. Organizations must obtain express consent (notice and opt-in) for the processing of financial data and implicit consent (notice and opt-out) for the processing of personal data. Express or written consent is required if an organization is processing sensitive personal data. Mexico has strong breach notification requirements. Security breaches must be promptly reported by data processors to data subjects.

Netherlands

The EU General Data Protection Regulation (GDPR) is a proposal that will unify data-protection laws across the EU with a single set of rules that replaces the existing 1995 Data Protection Directive. The GDPR aims to modernize existing privacy laws to meet the challenges of new technologies, strengthen individuals' rights while promoting the free flow of personal data throughout the EU and achieve consistent implementation of data-protection policies in all EU Member States, including the Netherlands.

New Zealand

The Privacy Act of 1993 established data-protection and privacy requirements for organizations that process personal data. The personal data collected must be needed for lawful purposes connected with an organization's work. Data subjects are given the right to access and correct their personal information. Although there are no mandatory breach notification requirements in New Zealand, data subjects may submit complaints to the privacy commissioner.

Nigeria

Data-privacy legislation in Nigeria is fragmented. There is no comprehensive legislative framework on the protection of personal data but rather industry-specific laws that provide some privacy-related protections. Data privacy is covered under the following laws: Section 37 of the Constitution of the Federal Republic of Nigeria, Section 23 of the Freedom of Information Act (FOI Act), the Child Rights Act, the Consumer Code of Practice Regulations (NCC Regulations), the National Information Technology Development Agency (NITDA) and the Cybercrimes Act.

Norway

Data-protection legislation in Norway consists of the Personal Data Act and the Personal Data Regulations. Norway's laws mirror the EU General Data Protection Regulation. Data processors must obtain a data subject's consent before processing their personal information. Data processors may only transfer personal data to other countries if those countries ensure an adequate level of protection.

Poland

The EU General Data Protection Regulation (GDPR) is a proposal that will unify data-protection laws across the EU with a single set of rules that replaces the existing 1995 Data Protection Directive. The GDPR aims to modernize existing privacy laws to meet the challenges of new technologies, strengthen individuals' rights while promoting the free flow of personal data throughout the EU and achieve consistent implementation of data-protection policies in all EU Member States, including Poland.

OPT-IN/CONSENT	RIGHT TO ERASURE	DATA TRANSFER
DISCLOSURE	ENFORCEMENT	ACCOUNTABILITY - PRIVACY BY DESIGN
BREACH NOTIFICATION	ACCESS	OPT-OUT

Portugal

The EU General Data Protection Regulation (GDPR) is a proposal that will unify data-protection laws across the EU with a single set of rules that replaces the existing 1995 Data Protection Directive. The GDPR aims to modernize existing privacy laws to meet the challenges of new technologies, strengthen individuals' rights while promoting the free flow of personal data throughout the EU and achieve consistent implementation of data-protection policies in all EU Member States, including Portugal.

Russia

Data-protection legislation in Russia consists of many provisions found in the Strasbourg Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data and the Personal Data Protection Act (DPA). There are also sectoral laws that regulate data processing for specific industries, such as the Russian Labor Code, Russian Air Code and Federal Law No. 323 on the Fundamentals of Protection of Health of Citizens in the Russian Federation.

Singapore

As in China, data-protection and privacy legislation in Singapore is highly influenced by the EU Data Protection Directive. Singapore's Personal Data Protection Act (PDPA) establishes a data-protection law that comprises various rules governing the collection, use, disclosure and care of personal data. It recognizes both the rights of individuals to protect their personal data, including rights of access and correction, and the needs of organizations to collect, use or disclose personal data for legitimate and reasonable purposes.

Slovakia

The EU General Data Protection Regulation (GDPR) is a proposal that will unify data-protection laws across the EU with a single set of rules that replaces the existing 1995 Data Protection Directive. The GDPR aims to modernize existing privacy laws to meet the challenges of new technologies, strengthen individuals' rights while promoting the free flow of personal data throughout the EU and achieve consistent implementation of data-protection policies in all EU Member States, including Slovakia.

South Africa

Data privacy and protection in South Africa is regulated by the Protection of Personal Information Act (PPI Act) as well as the Constitution of the Republic of South Africa. The PPI Act specifically imposes eight information protection conditions, namely, accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards and data-subject participation.

South Korea

The Personal Information Protection Act (PIPA) was enacted on September 30, 2011. Under the PIPA, data processors must obtain a data subject's consent for collection of personal information. The PIPA distinguishes between personal information and sensitive personal information. Organizations must obtain separate consent for collection of sensitive personal information.

OPT-IN/CONSENT	RIGHT TO ERASURE	DATA TRANSFER
DISCLOSURE	ENFORCEMENT	ACCOUNTABILITY - PRIVACY BY DESIGN
BREACH NOTIFICATION	ACCESS	OPT-OUT

Spain

The EU General Data Protection Regulation (GDPR) is a proposal that will unify data-protection laws across the EU with a single set of rules that replaces the existing 1995 Data Protection Directive. The GDPR aims to modernize existing privacy laws to meet the challenges of new technologies, strengthen individuals' rights while promoting the free flow of personal data throughout the EU and achieve consistent implementation of data-protection policies in all EU Member States, including Spain.

Sweden

The EU General Data Protection Regulation (GDPR) is a proposal that will unify data-protection laws across the EU with a single set of rules that replaces the existing 1995 Data Protection Directive. The GDPR aims to modernize existing privacy laws to meet the challenges of new technologies, strengthen individuals' rights while promoting the free flow of personal data throughout the EU and achieve consistent implementation of data-protection policies in all EU Member States, including Sweden.

Switzerland

The Federal Act on Data Protection (DPA) and its ordinances regulate Switzerland's data-protection and privacy legislation. Organizations that collect and process personal data must obtain consent from data subjects and inform them of the purpose of its processing. Data transfer to other countries is allowed if the destination country offers an adequate level of data protection.

Taiwan

Data protection in Taiwan is mainly regulated by the Personal Data Protection Law (PDPL). Under the PDPL, written consent is required for processing personal information. Breach notification requirements are enforced if personal data is breached due to violation of the PDPL. Data processors are obligated to inform data subjects of the purpose for personal data collection.

Thailand

Thailand does not have a data-protection and privacy legislative framework in place. Statutory laws for specific areas such as banking and financial businesses provide certain protections against the collection and processing of personal information. Thailand has no breach notification requirements. Certain provisions of the Child Protection Act B.E. 2543 (2003) protect the privacy rights of children.

Turkey

Data-protection legislation in Turkey is fragmented and consists of a number of provisions, several laws and regulations. Amendments to the Turkish constitution in 2010 made the protection of personal data an individual's right. Personal data may be processed under certain consent requirements. Other laws and regulations that protect personal data include the Civil Code, the Code of Obligations, the Criminal Code, the Law on the Right to Access Information, the Electronic Communications Act and the E-commerce law.

United Kingdom

Britain's recent decision to withdraw from the European Union has raised many concerns about the state of data-privacy legislation, especially as it relates to the EU General Data Protection Regulation (GDPR). The GDPR will impact any UK businesses that offer any services to the EU market, regardless of whether the UK is part of the EU. The GDPR is a proposal that will unify data-protection laws across the EU with a single set of rules that replaces the existing 1995 Data Protection Directive. The GDPR aims to modernize existing privacy laws to meet the challenges of new technologies, strengthen individuals' rights and achieve consistent implementation of data-protection policies in all EU Member States.

Uruguay

Data protection in Uruguay is regulated by the Data Protection Act Law No. 18.331 and Habeas Data Action (Uruguayan Law). Provisions within these laws address notification, consent, access and correction rights. Uruguay is considered by most to have one of the most comprehensive legislative frameworks.

If you have any further questions:

Jessie Kernan
EVP, Applied Data and Strategy
T: +1 (310) 563-7203
E: Jessie.Kernan@rapp.com

Addison Deitz
EVP, Director of Global Operations and Client Support
T: +1 (972) 409-5415
E: Addison.Deitz@rapp.com

Caleb Bernal
Consumer and Market Intelligence Coordinator
T: +1 (212) 817-6973
E: Caleb.Bernal@rapp.com

Devin O'Loughlin
Global Manager, Corporate Reputation
T: +1 (212) 817-6682
E: Devin.Oloughlin@rapp.com

References

Links for Further Reading

1. **"Joint Statement on the Final Adoption of the New EU Rules for Personal Data Protection."** European Commission, 14 Apr. 2016. Web.

   http://europa.eu/rapid/press-release_STATEMENT-16-1403_en.htm

2. European Commission. Press Release Database. **"Agreement on Commission's EU Data Protection Reform Will Boost Digital Single Market."** N.p., 15 Dec. 2015. Web

   http://europa.eu/rapid/press-release_IP-15-6321_en.htm

3. **"Different Types of Consent."** PrivacySense.net, n.d. Web.

   http://www.privacysense.net/different-types-consent/

4. Sherman, Chris, Enza Iannopollo, Heidi Shey, Merritt Maxim, Jennie Duong, Kelley Mak, Christopher McClean, Alexander Spiliotes, and Peggy Dostie. **Forrester's 2015 Data Privacy Heat Map.** Rep. Forrester, 13 Oct. 2015. Web.

   https://www.forrester.com/report/Forresters+2015+Data+Privacy+Heat+Map/-/E-RES61221

5. Rotenberg, Marc, and David Jacobs. **"Updating the Law of Information Privacy: The New Framework of the European Union."** Harvard Journal of Law & Public Policy 36.2 (2013): 605-52. Mar. 2013. Web.

   http://www.harvard-jlpp.com/wp-content/uploads/2013/04/36_2_605_Rotenberg_Jacobs.pdf

6. Hunton & Williams. **"Hunton & Williams Releases Guide to the Proposed EU General Data Protection Regulation."** Hunton & Williams, May 2015. Web.

   https://www.hunton.com/files/Publication/e148d184-7b15-4e62-b295-0febc750f64d/Presentation/PublicationAttachment/f0ccd336-9871-4fba-b0ee-9e4bee319d37/Hunton_Guide_to_the_EU_General_Data_Protection_Regulation.pdf

7. Hyams, Oliver, and Pupil Barrister. **"The Right to Be Forgotten."** Web log post. 1essexcourt. 1ecchambersblog, 15 May 2014. Web.

   https://1essexcourt.wordpress.com/author/1ecchambersblog/

8. European Commission. European Commission – Press Release. **"Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses."** Europa.eu. N.p., 25 Jan. 2012. Web.

   http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en

9. United States. Federal Trade Commission. **"Complying with COPPA: Frequently Asked Questions."** FTC, 20 Mar. 2015. Web.

   https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions

10. McCallister, Erika, Tim Grance, and Karen Scarfone. **"Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)."** Tech. no. 800-122. National Institute of Standards and Technology (NIST), Apr. 2010. Web.

    http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

RAPP