PAUL HASTINGS

COMPLIANCE CHECK – ARE YOUR PRIVACY AND CYBERSECURITY PRACTICES COMPLIANT WITH THE EUROPEAN UNION (EU) GENERAL DATA PROTECTION REGULATION (GDPR)?

PAUL HASTINGS

TABLE OF CONTENTS

OVERVIEW OF THE EU GDPR

The GDPR became effective on May 25, 2018 and applies to any company that intentionally offers goods or services to residents of the European Union, or that monitors the behaviors of individuals within the EU. It required companies to assess their privacy and cybersecurity practices like never before and to implement changes that to their data access, consent, data portability, and breach notification practices. It further required companies, in some instances, to appoint a data protection officer responsible for overseeing these often new and potentially challenging privacy and cybersecurity practices.

Since the GDPR went into effect, we have seen the resulting impacts on companies with regards to fines, small and large, related to GDPR compliance requirements, the increased privacy compliance budgets and staffing, and changes to employee codes of conduct and practices in conjunction with personal data of individuals.

As your company continues with its GDPR compliance activities, it is important to reflect, review, and assess how your data privacy and cybersecurity practices successfully meet the requirements of GDPR and where additional enhancements and improvements can be made to further your company's compliance posture.

GDPR COMPLIANCE CHECKLIST

1. **Awareness and Training**. Privacy and cybersecurity awareness and trainings are critical to ensuring not only compliance with data protection laws and regulations, but also the safety and security of personal data. Are your employees, contractors, and staff aware of and routinely reminded of the privacy and cybersecurity compliance requirements incumbent upon them to ensure safeguarding of personal data?

2. **Data Protection Officers**. If applicable, your company should have a designated individual responsible for data protection compliance. From time to time, it is appropriate to assess where this role sits within your organization's structure and governance arrangements. Where your company does not already have a Data Protection Officer ("DPO"), you should review whether circumstantial changes mean you are required to formally designate a Data Protection Officer and proceed accordingly. The following organizations must designate a DPO:

    - a public authority (except for courts acting in their judicial capacity);
    - an organization that carries out the regular and systematic monitoring of individuals on a large scale; or
    - an organization that carriers out the large scale processing of special categories of data, such as health records.

3. **Data Protection by Design and Data Privacy Impact Assessments**. This is the idea that privacy and cybersecurity considerations should be integrated into every stage and aspect of a new product or organizational structure at a company. Has this been consistently and effectively implemented at your company? A Data Privacy Impact Assessment ("DPIA") is designed to help you systematically analyze, identify, and minimize the data protection risks associated with a project or plan. Do your company's business units consistently and effectively utilize your DPIA processes and procedures?

4. **Record Keeping and Information You Hold**. Your company should be able to identify the categories, types, and locations of the personal data you collect and maintain regarding data subjects and be able to produce this information upon request in a timely manner. Do the processes and procedures you have implemented meet these compliance requirements? Further, personal data should be kept only for as long as it is required for the business purpose for which it was collected. Does your company have formal written policies for data retention? Does your company delete and/or destroy data when it is no longer needed?

5. **Privacy Notices, Cookies Policies, and Consent Procedures**. Your company's privacy notice(s) and cookies policies should be updated any time there has been a material change to your privacy and/or cybersecurity practices and at least on an annual basis. Your Privacy Notices should identify the lawful basis for your processing activities and you should ensure that consent mechanisms are managed and recorded appropriately. If your company engages in the processing of personal data regarding minors, you should also examine the age verification mechanisms and means of obtaining adult or guardian consent for such collection.

6. **Individuals' Rights**. Your company should review and assess on a regular basis whether your processes and procedures concerning individuals' rights are appropriate and inclusive of all rights afforded to data subjects under GDPR, including:

    - the right to be informed;
    - the right of access;
    - the right of rectification;
    - the right to erasure;
    - the right to restrict processing;
    - the right to data portability;
    - the right to object; and
    - the right not to be subject to automated decision-making.

7. **Data Subject Access Requests**. Your company should review the policies and procedures in place for responding to access requests from individuals on a regular basis and new or updated processes should be implemented as necessary. Integration efforts with other access request compliance requirements, such as those implemented for the California Consumer Privacy Act ("CCPA"), may also be appropriate if they have not already been accomplished.

8. **Cross-Border Transfers**. The GDPR requires certain contractual requirements for companies that engage in the cross-border transfer of personal data. Your company should review your standard template language on a regular basis to ensure it meets the requirements of GDPR. Where appropriate, it may be beneficial to implement usage of the Standard Contractual Clauses. It is important to note that the Court of Justice of the EU (CJEU) recently invalidated the EU-US Privacy Shield Framework. In addition, the European Data Protection Board (EDPB) recently published new Standard Contractual Clauses that will likely go into effect in 2021. It is important for companies to stay abreast of these developments and implement appropriate data transfer mechanisms as necessary.

9. **Processors and Vendor Management**. All companies that use external third parties or vendors to process personal data should have a third-party/processor management program in place that assesses and ensures compliance with data protection laws and applicable data transfer agreements. These assessments should be conducted at the beginning of the relationship and at least annually throughout the term of the third-party/processor agreement.

10. **Data Breaches and Notification**. All companies that engage in the collection and/or maintenance of personal data should have policies and procedures in place to detect, report, and investigate any suspected or actual personal data breaches. Your company should also have prepared resources to implement any data breach notification requirements, including the support of external vendors and/or outside counsel.

Where a company operates internationally and is subject to the privacy and cybersecurity compliance requirements of multiple jurisdictions, it may be appropriate to implement a cross-functional privacy business unit.

HOW THE PAUL HASTINGS PRIVACY & CYBERSECURITY SOLUTIONS GROUP CAN HELP WITH GDPR COMPLIANCE

Our Privacy and Cybersecurity Solutions Group operates under our Global Privacy and Cybersecurity Practice Group and is a unique blend of legal expertise and consultants that operate under the umbrella of the law firm. This provides two important benefits to the GDPR compliance services that we provide to clients: 1) Our work can be delivered under attorney-client privilege; and 2) Our recommendations have the weight and support of a respected, established, global law firm where we have reach-back capabilities to attorneys who have deep experience in U.S. and international legal issues in the areas of privacy and cybersecurity. Furthermore, as a leading law firm in the U.S., we have provided advice and support to hundreds of companies across all market sectors. The dynamic nature of our practice, which marries exemplary legal support with experienced consultants, means that we can help you operationalize the GDPR requirements while also providing you with an understanding of legal risk and exposure related to the law.

We can provide GDPR compliance support in any of the areas as listed above, and more specifically:

- **Document Review and Development**. We can enhance your current internal policies and procedures, as well as create new documentation to support your GDPR compliance program. Our team has extensive experience in creating program documentation that is both legally sufficient to meet regulatory requirements and customized to your unique business needs and functionality. We routinely work with clients to integrate GDPR compliance efforts into the broader compliance activities of the company and while we have a library of tried-and-true templates, we work closely with our clients to ensure that any documents we produce are usable, workable guidelines that their businesses can easily follow.
- **Compliance Gap Assessment**. Based upon the information provided above and our day-to-day experience in supporting GDPR compliance efforts at a broad range of companies, we can provide you with an easy-to-understand, actionable assessment that provides a clear picture of where your program is now compared to where you need to be to comply with GDPR and in comparison to other similarly-situated companies.
- **Remediation Roadmap Development**. Based on the compliance gap assessment, we can provide you with a prioritized, systematic guide for remediating those identified gaps, and provide guidance on who in your organization should be responsible for implementing each action item and what additional tools or resources you may need.
- **Data Mapping**. Our consultants are experienced at creating detailed data maps based on your documents and data collection, storage, sharing, and destruction practices. When necessary, we also collaborate with experienced technical firms to provide support for implementation and operationalization of data mapping tools.

PAUL HASTINGS

OUR TEAM

Jacqueline Cooney

Leader, Privacy and Cybersecurity Group
Washington, DC
+1.202.551.1236
jacquelinecooney@paulhastings.com

John Binkley

Senior Director, Privacy and Cybersecurity Group
Washington, DC
+1.202.551.1862
johnbinkley@paulhastings.com

Daniel Julian

Director, Privacy and Cybersecurity Group
Washington, DC
+1.202.551.1231
danieljulian@paulhastings.com

Brianne Powers

Director, Privacy and Cybersecurity Group
Washington, DC
+1.202.551.1237
briannepowers@paulhastings.com

PAUL HASTINGS

ABOUT PAUL HASTINGS

Paul Hastings provides innovative legal solutions to many of the world's top financial institutions and Fortune 500 companies in markets across Asia, Europe, Latin America, and the United States.

We offer a complete portfolio of services to support our clients' complex, often mission-critical needs—from structuring first-of-their-kind transactions to resolving complicated disputes to providing the savvy legal counsel that keeps business moving forward.

Since the firm's founding in 1951, Paul Hastings has grown steadily and strategically along with our clients and the markets we serve. We established successful practices in key U.S. and European cities, creating a broad network of professionals to support our clients' ambitions. In addition, we were one of the first U.S. law firms to establish a presence in Asia, and today we continue to be a leader in the region. Over the past decade, we have significantly expanded our global network of lawyers to assist our clients in financial centers around the world, including the emerging markets of Latin America.

Today, we serve our clients' local and international business needs from offices in Atlanta, Beijing, Brussels, Chicago, Frankfurt, Hong Kong, Houston, London, Los Angeles, New York, Orange County, Palo Alto, Paris, San Diego, San Francisco, São Paulo, Seoul, Shanghai, Tokyo, and Washington, D.C.

Drawing on the firm's dynamic, collaborative, and entrepreneurial culture, our lawyers work across practices, offices, and borders to provide innovative, seamless legal counsel—where and when our clients need us.

Ranked among the Top 5 on the A-List of the most successful law firms in the U.S. six years in a row

— The American Lawyer

Ranked among the Top 10 most innovative law firms in Europe and North America

— Financial Times' Innovative Lawyers Report

Named among the Top 5 for Overall Best Law Firm to Work For four years in a row

— Vault's Annual Survey

Connect with us to keep current on the latest legal developments.

PAUL HASTINGS

GLOBAL RESOURCES

21 OFFICES *ACROSS THE AMERICAS, ASIA, AND EUROPE*

1 LEGAL TEAM *TO INTEGRATE WITH THE STRATEGIC GOALS OF YOUR BUSINESS*

THE AMERICAS

Atlanta
Century City
Chicago
Houston
Los Angeles
New York
Orange County
Palo Alto
San Diego
San Francisco
São Paulo
Washington, D.C.

ASIA

Beijing
Hong Kong
Seoul
Shanghai
Tokyo

EUROPE

Brussels
Frankfurt
London
Paris

PAUL HASTINGS

THE AMERICAS

Atlanta
1170 Peachtree Street, N.E.
Suite 100
Atlanta, GA 30309
t: +1.404.815.2400
f: +1.404.815.2424

Century City
1999 Avenue of the Stars
Los Angeles, CA 90067
t: +1.310.620.5700
f: 1.310.620.5899

Chicago
71 S. Wacker Drive
Forty-Fifth Floor
Chicago, IL 60606
t: +1.312.499.6000
f: +1.312.499.6100

Houston
600 Travis Street
Fifty-Eighth Floor
Houston, TX 77002
t: +1.713.860.7300
f: +1.713.353.3100

Los Angeles
515 South Flower Street
Twenty-Fifth Floor
Los Angeles, CA 90071
t: +1.213.683.6000
f: +1.213.627.0705

New York
200 Park Avenue
New York, NY 10166
t: +1.212.318.6000
f: +1.212.319.4090

Orange County
695 Town Center Drive
Seventeenth Floor
Costa Mesa, CA 92626
t: +1.714.668.6200
f: +1.714.979.1921

Palo Alto
1117 S. California Avenue
Palo Alto, CA 94304
t: +1.650.320.1800
f: +1.650.320.1900

San Diego
4747 Executive Drive
Twelfth Floor
San Diego, CA 92121
t: +1.858.458.3000
f: +1.858.458.3005

San Francisco
101 California Street
Forty-Eighth Floor
San Francisco, CA 94111
t: +1.415.856.7000
f: +1.415.856.7100

São Paulo
Av. Presidente Juscelino
Kubitschek, 2041
Torre D, 21º andar
São Paulo, SP, 04543-011
Brazil
t: +55.11.4765.3000
f: +55.11.4765.3050

Washington, DC
2050 M Street, N.W.
Washington, DC 20036
t: +1.202.551.1700
f: +1.202.551.1705

ASIA

Beijing
Suite 2601, 26/F
Yintai Center, Office Tower
2 Jianguomenwai Avenue
Chaoyang District
Beijing 100022, PRC
t: +86.10.8567.5300
f: +86.10.8567.5400

Hong Kong
21-22/F Bank of China Tower
1 Garden Road
Central Hong Kong
t: +852.2867.1288
f: +852.2523.2119

Seoul
33/F West Tower
Mirae Asset Center1
26, Eulji-ro 5-gil, Jung-gu,
Seoul 04539, Korea
t: +82.2.6321.3800
f: +82.2.6321.3900

Shanghai
43/F Jing An Kerry Center
Tower II
1539 Nanjing West Road
Shanghai 200040, PRC
t: +86.21.6103.2900
f: +86.21.6103.2990

Tokyo
Ark Hills Sengokuyama Mori
Tower
Fortieth Floor
1-9-10 Roppongi
Minato-ku Tokyo 106-0032
Japan
t: +81.3.6229.6100
f: +81.3.6229.7100

EUROPE

Brussels
Avenue Louise 480
1050 Brussels
Belgium
t: +32.2.641.7460
f: +32.2.641.7461

Frankfurt
TaunusTurm – Taunustor 1
60310 Frankfurt am Main
Germany
t: +49.69.907485.000
f: +49.69.907485.499

London
100 Bishopsgate
London EC2N 4AG
United Kingdom
t: +44.20.3023.5100
f: +44.20.3023.5109

Paris
32, rue de Monceau
75008 Paris
France
t: +33.1.42.99.04.50
f: +33.1.45.63.91.49