PROCUREMENT AND ENFORCEMENT
OF INTELLECTUAL PROPERTY

TORRANCE
21515 Hawthorne Blvd.
Suite 200
Torrance, CA 90503-6501
(310) 405-7425

PASADENA
1055 East Colorado Blvd.
Fifth Floor
Pasadena, CA 91106-2327
(626) 204-9206

CISLO & THOMAS LLP
Attorneys at Law

12100 Wilshire Boulevard
Suite 1700
Los Angeles, CA 90025-7103
(310) 979-9190 Fax (310) 394-4477
www.cislo.com

WESTLAKE VILLAGE
2829 Townsgate Road
Suite 330
Westlake Village, CA 91361-3006
(805) 496-1164 Fax (805) 435-8446

PATENT, TRADEMARK
COPYRIGHT & RELATED MATTERS

SANTA BARBARA
7 West Figueroa Street
Third Floor
Santa Barbara, CA 93101-5109
(805) 962-1515

SAN DIEGO
12636 High Bluff Drive
Suite 400
San Diego, CA 92130-2071
(619) 481-5448

DATA PRIVACY AND CYBERSECURITY COMPLIANCE

The California Consumer Privacy Act ("CCPA") and the General Data Protection Regulation ("GDPR") are privacy regulations protecting consumers in California and the European Union, respectively. These regulations ensure that consumers' personal information is protected and that the information collected by businesses is only collected for the purpose intended. Today businesses are often required to comply with both the CCPA and the GDPR.

Listed below are a number of items that should be considered when reviewing your CCPA compliance.

Notice at or Before Time of Collection

Your privacy policy must be accessible on your website and is required to inform users of your services, their rights, and what information will be collected from them "at or before the time of collection." This notification can take many forms but most often is in the form of a banner that pops up when a website or application is loading, linking the user to the company's privacy policy.

Keep Data Inventories Updated and Update Policies Accordingly

Another requirement of the CCPA is that businesses make sure that their data inventories continue to be updated. When things change in the data inventory, we recommend that you note such changes in the attached table of information so you can track such changes.

In addition, when processes are updated, new technical systems are implemented, or any change happens to the way you collect or use personal information, we recommend that you make these modifications in the data inventory as well. If you do make changes such as the ones described above, your privacy policy will need to be updated. Pursuant to the CCPA, your privacy policy must be updated at least once every 12 months.

Consumer Requests

Under the CCPA, California residents now have the right to know what personal data is being collected; whether their data is being sold and to whom; say "no" to the sale of their information/data; access their data; and request businesses delete any information collected about

them. It is required that businesses have a way to authenticate that the requests are legitimately from the customer and to respond to any such requests in a timely manner.

Option to Opt-Out of Sale of Information Requirement

If your business ever begins to sell consumer information, it is also a requirement under the CCPA that businesses must provide a specific link on the home page that states "Do Not Sell My Information" giving the consumer the ability to opt-out of the sale of such information. If consumers do opt-out, they cannot be asked to re-consent until 12 months have passed since the opt-out.

Reasonable Security Standard

Businesses must protect consumer information with "reasonable" security. It's important to keep up to date on security standards and possible new security solutions over time. When trying to determine what is "reasonable," it may be helpful to think about the different types of information that your company collects from your data inventory. This will make it easier to determine which collected information is the most sensitive.

Personal information such as names and phone numbers are not nearly as sensitive as social security numbers, health information, or financial information. If your company does collect information that is extra sensitive, it is a good idea to encrypt this information. It is also good practice to encrypt consumer passwords, if stored, as well.

Please keep in mind that there may be penalties if the "reasonable" security standard is not complied with. If your company becomes the victim of a cyber-attack and "non-encrypted or non-redacted" personal information is exposed to the hacker, consumers may have a right to sue your business. This can quickly become very expensive and devastating to your company.

Third Party Contracts

Lastly, CCPA compliance applies to third-party agreements. If you collect information from consumers and share such information with a third party, of any kind, you will need to memorialize the terms upon which the third party must handle the data that you have shared. The terms of the agreement must be the same as the terms that consumers were informed of in your company's privacy policy. A new section should be added to your third-party contracts, if this hasn't been done already, requiring them not to exceed the scope of use as described in your company's privacy policy.

Note, if you begin selling information to third parties, you will need to require that the third party also implements a process to handle consumer privacy requests, as well as provide an opt-out link stating "Do Not Sell My Information."

DATA PRIVACY AND CYBERSECURITY CHECKLIST

The following is a checklist to help your company with intellectual property issues to investigate or protect. For additional information, please visit our website at www.cislo.com and use our IPINFO, IPSEARCH and IPNEWS tabs for links to numerous IP resources. Please feel free to call us for an appointment to discuss your situation.

Data Privacy

___ Start data mapping—i.e. keeping track of the type of data your business collects and/or uses and how this data is being stored.

___ Check to see if your business falls under prevalent privacy laws, such as the California Consumer Privacy Act (CCPA) and/or the General Data Protection Regulation (GDPR). For example, US-based businesses that typically fall under the GDPR are in industries such as e-commerce, logistics, software services, and/or travel. In regards to the CCPA, a business that derives 50% or more of its annual revenues from selling California consumers' personal information will need also need to comply, among other requirements.

___ Implement a clear process for an individual to opt out of selling personal information (CCPA).

___ Put a system into place to handle the individual rights of disclosure, access and deletion (CCPA).

___ Consult with an attorney to ensure you are in ongoing compliance with the constantly evolving privacy regulations.

___ Prepare for the future by keeping up to date with all U.S. privacy laws and regulations as more states follow lead to California.

Cybersecurity

___ Be prepared for an unexpected data breach or security incident by having an internal Incident Response Plan (IRP).

___ Identify and assess cybersecurity risks and threats; identifying vulnerabilities will provide a framework to minimize the risks and effects of a cyber-attack.

___ Prioritize employee training and awareness programs since the majority of cyber incidents are caused by employees inadvertently clicking on phishing e-mails.

___ Implement internal password policies—IT policies should mandate complex passwords and require personnel to periodically change their passwords.

___ Use Two-Factor Authentication to provide an additional layer of security.

___ Update operating systems and antivirus programs to enhance internal security mechanisms.

___ Utilize filtering tools to minimize the risk of phishing e-mails.

___ Screen potential employees and contractors before assigning work involving sensitive or confidential data.

___ Backup data on a regular basis to prevent unnecessary loss.

___ Consider purchasing cybersecurity insurance in the event of a data breach, which may cover the liabilities associated with data breaches in part or in full.