Issue: March, 2018

Global Directors Beware: Are You Ready for EU's Data Protection Regulation?

On May 25, 2018, the European Union (EU) General Data Protection Regulation (GDPR) will go into effect in the 28 EU member states. Companies, the world over, are now rushing to meet the deadline for compliance but how many will make it?

The GDPR requires every organization that offers products or services to EU residents comply with a strict set of data privacy and security measures. These requirements will apply equally to those companies' business partners. This essentially results in global regulation with potentially financial penalties and even criminal penalties for non-compliance.

GDPR is not just an EU-specific regulation – every EU citizen's private data, regardless of where it is stored, must be protected. In today's world of web-connected businesses, even small organizations not located in the EU may have data for individuals from EU countries and are, therefore, subject to aspects of GDPR. Storing the personal data of just one EU customer means that compliance with GDPR is required.

While originally thought to bring uniformity to enforcement in the EU, some EU member states are already making efforts to differentiate applicability of GDPR in their countries, which could add to the difficulties of implementation. As it stands and was enacted, GDPR is binding on all EU members and, at 88 pages, is designed to address the disruption to data privacy wrought by the rapid evolution of information technology and business models over the past 20 years. The regulation will be enforceable by the data protection authorities (called "supervisory authorities") of member states. Multinational companies, with their greater access to resources, will likely be able to meet immediately some of the GDPR's requirements, but most will find that they need all the available time before inception to be completely ready. On the other hand, it is anticipated that many smaller entities may not be GDPR compliant before the deadline.

The GDPR will replace the EU's existing data privacy and security regime, the Data Protection Directive 95/46/EC, which was enacted in 1995. The penalties for the violation of privacy regulations under the existing regulation vary among member states, with the potential for fines ranging from €150,000 to €900,000 ($184,540 to $1.1 million). Supervisory authorities had little recourse against large, well-funded multinationals that viewed such fines merely as a cost of doing business. This changes under the GDPR, which could see fines imposed up to €20 million ($24.6 million), or 4 percent of the offending company's global annual revenue, whichever is higher. GDPR also provides for potential criminal prosecution to be sought against directors and officers for deliberate breaches. Simply put, a board member can be jailed.

The regulation also features notification requirements modeled loosely after U.S. breach notification laws – the biggest difference being a new, shortened 72-hour time frame. Given that most breaches are not immediately discovered, and the extent of a breach can take time to determine, this could be a challenge for many entities. Because the U.S. does not have a federal data protection law, data protection measures are set forth in numerous state laws and regulations. As a result, with the advent of the GDPR, organizations based in the U.S., which hold data on European customers, now have the daunting task of keeping track of each U.S. regulation, while ensuring that they are compliant with GDPR.

Fortunately, the GDPR's requirements for data protection are in concert with most regulations in the U.S. There is nothing in the National Institute of Standards and Technology (NIST) Cybersecurity Framework that conflicts with the data protection practices required by GDPR.

An organization's CEO and board of directors are responsible for GDPR compliance as well as with compliance with U.S. laws. They must ensure that practices are balanced with all cyber security and data privacy regulations that apply to their organization. Rather than passively relying on others to understand the issues and resolve them, the board must become more involved and should start by asking questions about their organization's level of readiness for GDPR and consider allocating resources to ensure the company is compliant by the deadline. Unfortunately, most boards are not cyber-savvy. An article in the Harvard Law School Forum on Corporate Governance and Financial Regulation strongly suggested that the board itself create a committee focused on cyber risk and cyber security that covers the gamut of potential threats from both internal and external parties, including strong data protection capabilities. The article makes it clear that directors need to deal in specifics, rather than an "overview" approach. A report published by Accenture revealed that only 6 percent of the directors at the world's largest financial institutions have technology expertise. The data in North America is hardly better, with only 12 percent of directors having a professional technology background, according to the report. Clearly, boards of businesses large and small are going to have to build or acquire new cyber-security skills going forward.

It is unlikely that the focus on holding individual directors responsible for cyber security will abate. Data breaches which are reported almost daily have raised the general level of distrust of "big business," such as the recent criticism of the officers of EquiFax and Uber and many others before them, and a corresponding increase in the desire to hold top executives personally responsible. In response to these trends, board members must increase their cyber security skills, engagement and awareness to comply with the GDPR and the likely next wave of cyber laws and regulations.

Not only is GDPR of interest to multinationals and their U.S. business partners, but underwriters of cyber liability and management liability insurance policies are looking at how it will increase market opportunities. First, however, underwriters will want to be confident that their insureds are making timely strides toward compliance. If companies fail to comply, they could be slapped with significant penalties, and face reputational damage. At the same time, unhappy shareholders could sue the directors and officers of such organizations for securities losses. Multinationals and their US business partners can expect to have to answer underwriters' queries as to their compliance with GDPR when they are buying or renewing their cyber liability and management liability policies for the next several years.

As organizations approach the inception date of GDPR, they face the challenge of becoming compliant with the new regulations while at the same time dealing with potential conflicts with U.S. laws. A portion of the GDPR will remain in flux as some member states make an attempt to differentiate applicability of GDPR. This will continue to cause uncertainty until and if the European Commission decides to step in and require absolute uniformity among the members.

Meanwhile, it would be a good idea for companies and their data processing officers to develop relationships with the supervising authority in each EU state where they do business. Having a relationship and evidencing a desire to comply with the GDPR may persuade a regulator that a minor failure to comply is insignificant.

Only time will tell how the regulations will be enforced by EU supervising authorities and European courts. There is no doubt, however, that it will be quite uncomfortable to be the "first" to be publicly targeted for violation of the GDPR.

Source: *https://www.insurancejournal.com*

Insuring Products of the Mind

The rapid growth in patent infringement litigation in 2013 – almost 6,500 cases, or an increase of 25 percent over 2012, according to PricewaterhouseCoopers – might appear to be a strong motivator for at-risk businesses to buy intellectual property insurance. But the complicated world of IP and the insurance market that covers this unique class has yet to overcome long-standing barriers to buying, the experts say. That's not to say opportunity doesn't exist in this niche.

"One of these days this market is going to break," says Richard Betterley, president of Betterley Risk Consultants, an independent consulting firm specializing in risk management that publishes The Betterley Report.

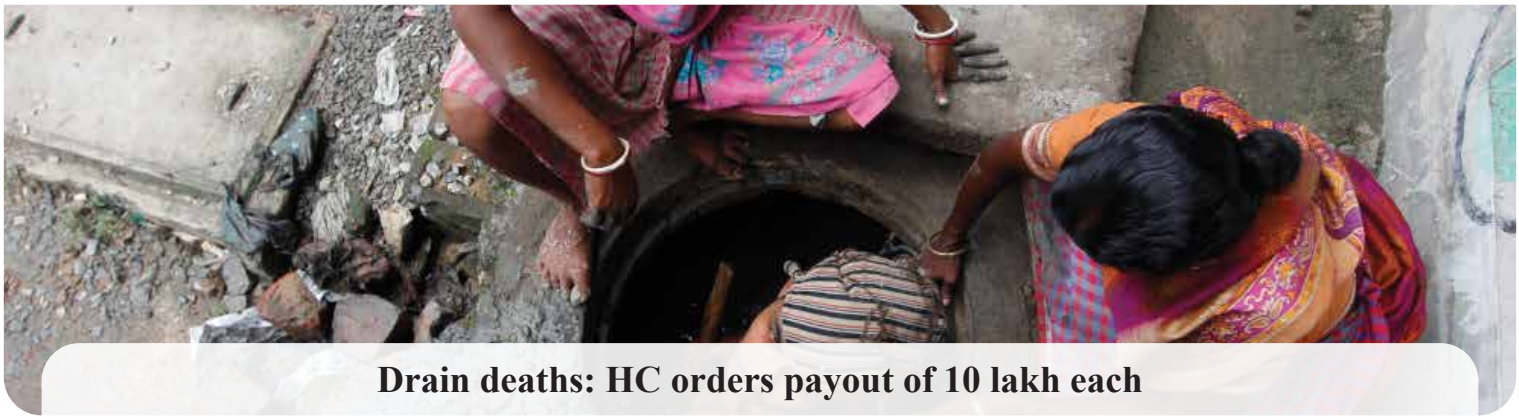
"This market has been really tough [but] it should be huge," says Graeme Newman, director, CFC Underwriting. Intellectual property insurance should be a mainstream product, he says.

There have been energetic attempts to grow the intellectual property insurance market. But so far, those attempts have not created much market expansion. Only a handful of IP coverage sources exist today. According to The Betterley Report's "Intellectual Property and Media Liability Insurance Market Survey 2014," only four carriers play in the IP space, some more than others: AIG, Liberty Mutual, Lloyd's (via Intellectual Property Insurance Services and SAMIAN) and ThinkRisk (Aspen). But Betterley, and other IP market experts believe it's only a matter of time. Everybody's at risk when it comes to intellectual property exposures, says CFC's Newman. CFC Underwriting, based in London, is a Lloyd's managing general agency specializing in insurance products for specific niche markets. Everybody has some form of intellectual property and everybody risks infringing on others' intellectual property, Newman says. "This should be a huge global market." The lack of market growth can be traced in part to challenges insurers have with underwriting IP risks profitably, the experts say. The complexity of defining intellectual property is a challenge to insurers, according to Robert Fletcher, president of Intellectual Property Insurance Services Corp. (IPISC), and the originator of the first-ever intellectual property infringement abatement policy. "If you go back and you look at history, we have been insuring products of the hands – homeowner's, and fire, automobile, even perhaps health insurance – all of that is not difficult to define," Fletcher says. "But when you get into 'products of the mind' – patent, copyright, trademark, trade dress and trade secret coverages – you are talking about something that's more difficult to define." That ambiguity causes people to ask, "Well, what is it you really want to have insured?" And that's a big challenge, he says. That challenge isn't helped by the lack of industry expertise in the field of insuring intellectual property, according to CFC's Newman. "The insurance market has been battling for decades with how to write this coverage effectively," he says. The market hasn't grown because there are so few people with the right level of experience to underwrite the class. "That's been a real inhibitor." Betterley says that few agents and brokers have invested time needed to learn about IP exposures and how to cover them. "Brokers don't really understand the topic or coverage; therefore it's very difficult for the prospective buyer to feel confident that, yes, this is something I should buy," Betterley says. There is another reason insureds choose not to buy: it's often easier for defendants to simply pay-off "patent trolls" than it is to fight them. "Patent trolls," or Patent Assertion Entities (PAEs) and Non Practicing Entities (NPEs), are firms that own patents but do not make products from them. While there are differences between the two, both are sometimes referred to as "patent trolls" because they are seen as exploiting technological advances that make it difficult to establish boundaries for patents and they use aggressive litigation tactics

against target companies, such as threatening to sue for patent infringement without specific evidence. In June 2013, the Obama Administration reported that suits brought by PAEs had tripled in the previous two years and the costs from litigation grew to almost $13 billion. More than 100,000 companies were sued by PAEs in 2012 alone, according to the "Patent Assertion and U.S. Innovation" report, published by the Office of the President.

"It's an odd combination where the insureds think on the one hand, 'I'm never going to have a problem so why do I need the insurance,'" Betterley says. "On the other hand it happens so frequently, 'I'll just write a check and make the non-practicing entity claims go away; it's cheaper than having the insurance company involved,' which doesn't make sense." RPX Patent Infringement Liability Insurance reimburses legal costs and some settlement costs incurred by operating companies in litigations initiated by most NPEs. The base policy provides limits of up to $5 million annually to cover litigation costs incurred to defend against patent infringement suits brought by NPEs in U.S. federal district court (International Trade Commission actions are excluded from the coverage, as are intellectual property indemnification obligations). The policy also can cover costs associated with re-examinations and declaratory judgments. Each policy carries a self-insured retention between $50,000 and $500,000. Policyholders must be members of the RPX client network.

Source: *https://www.insurancejournal.com*



Drain deaths: HC orders payout of 10 lakh each

The Delhi High Court has directed Delhi State Industrial and Infrastructure Development Corporation Ltd (DSIIDC) to pay 10 lakh compensation each to the families of two manual scavengers who died while cleaning a sewer in Bawana Industrial Area here in 2011. The court said the DSIIDC, which is responsible for developing and providing industrial infrastructure facilities, should have taken necessary steps to ensure that sewers are not opened for cleaning purposes by anyone. Justice V. Kameswar Rao said any mishap suggests a lapse on the part of the DSIIDC and directed it to pay the amount to the wife and mother of victims Tilak Ram and Bhagwan Singh respectively within three months. "In view of the prohibition, the DSIIDC should have taken necessary steps to ensure that the sewers are not opened for cleaning purposes by anybody. Any mishap occurring surely will suggest a lapse on the part of DSIIDC," Justice Rao said. "Moreover, the grant of compensation will not await a decision as to who was negligent to compel the deceased persons to go into the sewer lines. The liability being strict, this court is of the view that the DSIIDC shall pay an amount of 10 lakh each to the petitioners [families]," the judge said. It, however, granted liberty to DSIIDC to claim the money from the person who will be held guilty for the crime in the FIR registered in October 2011. According to the families, the victims had stepped into a blocked sewer for cleaning but lost consciousness after inhaling gases in the duct due to non-supply of safety equipment, masks and oxygen cylinder by the contractors, and died on the spot in 2011. The families added that the victims were the sole breadwinners and that they have been living in poverty after Mr. Ram and Mr. Singh's deaths. The court noted that there was "complete prohibition from engagement or employment for hazardous cleaning of a sewer or a septic tanks" under the Prohibition of Employment as Manual Scavengers and Their Rehabilitation Act. The court rejected the plea of the DSIIDC that neither it nor any of its contractors had engaged the two victims for cleaning of the sewer lines. It said this will not absolve it of the obligation to pay compensation if a person dies cleaning the same and noted that unfortunately, the authorities have denied their obligation to pay damages. "The compulsion of the dead persons was to earn some remuneration and having died in the course of earning remuneration, someone must be held responsible for the negligence, which resulted in their death," the court said.

Source: *http://www.thehindu.com*

J. B. BODA GROUP

- J. B. BODA - First on Protection – 70 Years of Transformation.
- Service with Commitment – Third Generation & Moving on …
- 24 Offices in India & 5 Offices Overseas in U.K., Singapore, Dubai, Nepal, Kenya.
- Employs 1,000 + personnel.

SERVICES

- Insurance & Risk Management Consultants, Life Valuation, Life & Employee Benefit Schemes.
- Actuarial Valuations.
- Training Academy.
- Valuation of Land, Building, Plant & Machinery.
- Protection & Indemnity Insurance Services.
- Fire, Engineering, Miscellaneous Accident Surveyors & Loss Assessors.
- Marine Cargo Surveyors, Loss Assessors, Superintendents.
- Container Surveyors, Tank Calibrators, Samplers & Analysts.
- International Reinsurance Brokers (Non-Life & Life).
- Direct Insurance Brokers (Non-Life & Life).

For more details email us at tenet@jbbodagroup.com

Address: J. B. Boda Reinsurance Brokers Pvt. Ltd. Maker Bhavan No. 1, Sir. Vithaldas Thackersey Marg, Mumbai 400 020, India | Phone :+91-22-6631 4949

www.jbboda.net | company/jb-boda | https://www.facebook.com/jbboda