FI Observer: Data Protection Law implications for Directors and Officers of Real Estate Investment Trusts (REITs)

You will no doubt have read about the two fines, amounting in total to £280 million, to be imposed on high profile corporations in relation to data breaches*. Global concerns about the privacy of data have intensified in the wake of the UK Information Commissioner's Office (ICO) statements of intent issued on consecutive days this month. As a result, directors and officers (D&Os) of corporations are looking to re-evaluate their liability outside of the scope of the traditionally evaluated personally identifiable information (PII) record count.

The whale of privacy laws – Europe's General Data Protection Regulation (GDPR) – was put into effect May 25, 2018, launching broad ranging implications for businesses upon its implementation, along with a looming threat of steep consequences for non-compliance.

Property owners, not least public organizations using the Real Estate Investment Trust (REIT) structure are particularly affected by the increasing focus on data Privacy laws. We explore the basic liability points that should be on all real estate management teams' radar.

1. US Legislation

Since May 2018, several US states have enacted their own version of data protection laws, many of which mirror the consumer requirements found in GDPR. While the California Consumer Privacy Act of 2018 has been widely deliberated, the 2019 Maryland Personal Information Protection Act is particularly significant for REITs, which are majority incorporated in the state.

The application of the personal data protection framework differs by industry, but the consequences are the same. Privacy and data protection laws expand D&O liability by placing new responsibilities for directors and officers, and larger obligations on organizations. Because of the far-reaching wording of the various legislation (pertaining to personal data of data subjects based in the jurisdiction, regardless of location), REITs must comply with the most rigorous rules of each privacy law.

"Data Subjects" for REITs might include:

***UK Information Commissioners Office - statements of intention to fine dated 8 and 9 July 2019**

Willis Towers Watson

Additional responsibilities for REIT boards and executive teams are ushered in by the introduction of a new supervisory role under GDPR, a "controller" who is responsible for determining both the means of processing and the purpose for personal data collected by the company. The role "processor" is also defined as a person who processes said personal data on behalf of the controller.

As the outlined requirements for "controllers" add additional duties for D&Os, it significantly increases personal liability in the event that a data privacy breach causes a financial loss. By mandating demonstration of compliance, communication with data subjects, strict time-constrained notification processes around breach reporting and appointment of vigorous processers, GDPR has given plaintiffs' lawyers a new laundry list of items to cite in litigation against the company and its management team following a breach.

2. Directors' Responsibilities

To prepare their D&Os for the new responsibilities of these burgeoning data laws, REITs need to reconsider the extent to which they control and process personal data.

Whose personal data is impacted by this?

What are the types of personal data that REITs will likely be processing?

What are the different purposes for the data which may be processed?

From a property owner's perspective, some examples of how operational nuances of REITs extend to collected personal data are outlined below:

Employee Data

- Extends from all applicants considered for the hiring process - resumes, personal contact details, background check information to sensitive information pertaining to current employees, like bank account details held for direct deposit, medical information, or performance records.

Investor Data

- Extends from individual investor or shareholder data, like investor lists, PII for directors of corporate investors, any data acquired in the process of credit or anti-money laundering checks.

Third Party Data

- Portfolio company data
- Joint venture data
- Management company data

3. How can REITs mitigate this expanding D&O liability?

The new data privacy laws, with their broad reach and uncharted territory, presents a difficult obstacle for REIT directors and officers: how to comply with uncertainty. A surge of event-driven lawsuits, following disruptive events like data breaches, have changed the quality and tenor of how REIT D&O litigation is filed. The impact of the new regulation on D&O settlements remains to be seen.

What can REITs do in the meantime? Cyber-security concerns and disclosures should be prioritized at the highest level of the organization, starting with the board. In response to new regulation, data privacy compliance is now a concern for each facet of the REIT, from the management team to employees to partner, vendor, and large tenant oversight.

There is case precedent for cyber-security vigilance, seen in a 2014 derivative action filed against Wyndham Worldwide, which alleged inadequate cybersecurity and deficient public exposures in the aftermath of a data breach.

The derivative action was dismissed where the board had proactively addressed cyber risks and exposures. Looking back on this with a 2019 perspective, would plaintiffs have been able to use violations of GDPR to better establish their case if regulation had been in place?

REITs are also in the unique position where their stock prices react to disruptive events effecting large tenants and utilized management companies. D&O underwriters have expressed concerns about shareholder backlash from third-party cyber events that could potentially impact rent payment, occupancy, or public perception concerns.

4. Understanding REIT D&O Policies for Privacy-Related Losses

While the cyber insurance product was developed to insure first-party and third-party exposures for companies, D&O liability resulting from cyber breaches should be addressed within the D&O policy now, in advance of a potential increase in cyber-related D&O claims.

Things to consider with regards to insurance:

- Are your policy limits sufficient to cover D&O privacy-related losses? Are you evaluating this question beyond traditional benchmarking and using analytical tools?
- Does the definition of "Wrongful Act" contemplate data privacy law violations?
- Does the definition of "Insured Person" contemplate controllers as defined by GDPR or similar laws?
- Are there any pertinent exclusions?
  - Public D&O policies should not have cyber exclusions (private companies may see these type of exclusions, but consider carve backs to protect individual D&Os)
  - Review Dedicated Side A protection for any company for any cyber-exclusions
  - Careful attention should be paid to the Bodily Injury & Property Damage Exclusion
- Have you weighed the pros and cons of having the same lead insurers for D&O and Cyber?

Privacy data liability concerns extend far beyond companies with traditional retail customer bases. While it is imperative that all REIT D&Os fully comply with the requirements of data privacy legislation to avoid the potentially costly consequences, management teams should carefully consider what insurance is in place to protect the D&Os against expensive law-suits and reputational damage.

Contact

Clare McCarrick
t: +1 212 915 8099
e: clare.mccarrick@willistowerswatson.com

Clare is a member of the WTW Global Finex Financial Institutions team, specializing in insurance solutions for Real Estate Investment Trusts

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 45,000 employees serving more than 140 countries and markets. We design and deliver solutions that manage risk, optimise benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas – the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

willistowerswatson.com/social-media

FPS667 WTW-FINEX 417901/09/19

willistowerswatson.com

Willis Towers Watson