ACREL News & Notes
November 2018

PropTech Privacy and Data Protection in the Age of the GDPR

Federica De Santis, Minta E. Kay, Karen Neuman, Gretchen Scott, Brenda Sharton,
Goodwin Procter LLP

Traditionally, privacy and data protection has not been a focus across the commercial real estate ("CRE") sector. However, with technological innovations and new business models driving change into the sector under the buzzword "PropTech", suddenly privacy has become relevant, and indeed critical, to maximising these business opportunities.

Smart buildings filled with sensors, technology and automation for crime prevention, energy efficiencies and sustainability are now a feature of CRE in major cities around the world. Landlords embed technology in their buildings that enables tenants to embrace flexible working practices and retailers are benefitting from location-driven technologies that provide powerful marketing and advertising opportunities. We are now moving to tech-driven smart city projects that promise to achieve new standards of sustainability, mobility, and economic opportunity. These projects are all backed by IoT and cloud infrastructures, artificial intelligence and big data analysis. They offer exciting ways to connect infrastructure, devices, objects and people and drive efficiencies into the way real estate projects are build, managed and operated.

Data capture is an inherent feature of such technological developments. Personal data is being collected, combined and used by landlords, tenants and other interested parties in increasingly opaque and complex ways. This, in turn, raises important questions as to the impact of technology on individuals' right to privacy. Perhaps inevitably, commercial interests and the right to privacy will conflict. Earlier this month, the privacy consultant appointed to Toronto's innovative tech-driven smart city project resigned, describing it as a "City of Surveillance", sparking concerns over the use of residents' data and behavioural monitoring through the technology embedded in such projects.

Privacy and data protection is currently high on the regulatory agenda due to these concerns. Laws are being passed in California and there is a growing call, including amongst big tech, for a federal privacy law. The global gold standard in privacy, however, is the European General Data Protection Regulation ("GDPR"), which came into full effect earlier this year. The GDPR has extraterritorial effect so is relevant for all businesses in the CRE sector that touch Europe. This article considers the GDPR and its impact on business in the CRE sector.

THE GDPR

The EU General Data Protection Regulation 2016/679 came into effect across the member states of the European Union (EU). The GDPR has introduced enhanced obligations on companies dealing with personal data (including non-EU established entities in certain circumstances), whilst giving individuals greater control over their data.

The GDPR aims to put the individual data subject in the driver's seat by giving them control over their personal data through transparency and the grant of individual rights -- together with a suite of other mechanisms, including extensive record keeping and data governance

requirements for entities that process personal data; investigatory and enforcement powers for authorities; and regulatory fines and damage awards in private litigation.

Every business within the CRE sector that targets the EU – including investment vehicles, real estate owners, property and asset managers – needs to appreciate the impact of the GDPR on their respective businesses.

The GDPR introduces a competition-like sanction regime with potential fines for violation of core data protection requirements (including processing without valid consent, breach of individuals' rights, or unlawful data transfers) of up to the higher of 20 million euros or 4% of global annual revenues, or up to the higher of 10 million euros or 2% of global annual revenues for violations regarding notification of data breaches, data processor terms, and other requirements.

The regulators have not been slow to use their new powers. The Dutch, UK and French authorities have launched investigations into GDPR compliance by certain businesses in what appears to be a series of targeted enforcement actions. The UK's ICO has banned a Canadian company from processing personal data of UK data subjects. The Austrian data protection regulator issued a relatively low fine against a retailer for the breadth of images captured by the retailer's CCTV camera. The European Data Protection Supervisor recently indicated that he expects to see more fines issue by year-end, along with warnings, and the imposition of remedial and other measures.

Moreover, non-profit organizations have embraced their new powers to bring claims on behalf of data subjects. The potential for collective actions (which are often compared to US-style class actions, although in practice they do not have the same potency) was brought into sharp focus when the consumer non-profit organization noyb.eu (run by privacy activist, Max Schrems) filed complaints against Google, Facebook, Instagram, and WhatsApp as soon as the GDPR come into effect.

Individuals are more aware of their rights than ever before and have not been reluctant to exercise them. Since May 25, businesses have been inundated with data subject access, deletion and other requests and EU authorities have received several complaints. In the US, a group of shareholders brought a class action against Nielsen Holdings for failing to properly disclose the impact of the GPDR to shareholders.

These factors all change the landscape for data protection, and require an entrenchment of training, policies, and practices designed to implement "privacy by design" and "privacy by default" throughout a business, and ensure greater transparency and accountability.

1. DOES IT APPLY TO OUR BUSINESS?

The GDPR applies to businesses "established" in the EU, as well as to non-EU businesses whose processing activities are related to the offer of goods or services to EU data subjects, or monitoring their behavior, wherever the processing (e.g. storage) takes place.

EU based affiliates of US companies will be subject to the GDPR wherever the data processing activities take place. For businesses that have no EU establishment, the application of the GDPR requires a case-by-case assessment. The core test is whether the non-EU business is carrying out processing that is related to an offer of goods or services to EU data subjects. So, business located outside the EU who process personal data in relation to asset management

services, CRE investments, leasehold or fee interests in real estate or other goods or services offered to individuals in the EU will be subject to the GDPR. By way of example, a US based landlord that offers rental accommodation to EU tenants will be subject to the GDPR in relation to the processing of the tenant data.

It is clear from the GDPR recitals that an offer includes not only an actual offer, but also the mere contemplation of an offer. There are also some important and untested nuances around this test in the context of the CRE sector. For example, can it be said that a landlord whose property is only offered to corporate tenants is making any offer to data subjects? Guidance is expected from the EU Data Protection Board on the scope of the extraterritorial application of the GDPR.

Tip: Every business within the CRE sector should assess the extent to which the GDPR applies to its business operations and to those of its affiliates. Keep a watch for upcoming EU guidance on the territorial scope of the GDPR.

2. CONTROLLER OR PROCESSOR?

As a threshold matter, the GDPR distinguishes between data controllers (the entity that makes the decisions related to the processing of personal data) and data processors (service providers that process data on behalf of a data controller). These distinctions are crucial because compliance obligations flow from the status as one or the other. Most of the GDPR's obligations fall on controllers.

Although there are certain presumptions around these roles, there is no immovable or settled determination as to whether an entity is a controller or processor; it is a factual test based on whether a business determines the purposes and means of the processing, or whether it is processing personal data on behalf of a controller. For example, an asset manager or a property manager may be a data processor on behalf of the landlord, or an independent controller or joint controller with the landlord depending on the degree of autonomy it has in relation to the processing of the relevant data. Relevant factors to establish the role include the level of instructions given by the landlord, the controls and oversight over the relevant activities and the expectations of individuals (e.g. tenants) as to who controls their data.

The GDPR contemplates the possibilities for entities to act as joint controllers. This will occur if two or more companies jointly determine the purpose and/or means of processing the same pool of data (even if the participation of the parties to the joint determination is not equally shared). According to EU authorities' guidance and recent EU case law, the test for joint controllership is broad and includes whether a business is facilitating the processing of personal data by another business (including in the content of intra-group relationship). The GDPR requires joint controllers to enter into a transparent arrangement that allocates their respective compliance responsibilities and are jointly and severally liable for each other's non-compliance. It is often difficult to draw the line between independent data controllers and joint data controllers, and a careful consideration of the conditions of collaboration between the parties is required.

Tip: Every business within the CRE sector that handles personal data must assess whether it is a controller, a joint controller or a processor in respect of that data, and clearly identify these roles in privacy notices provided to individuals.

Whichever role a business takes, there are significant responsibilities for both controllers and processors that, in most cases, will fundamentally change how a business processes personal data and how it works its partners and service providers.

3. REVIEWING PRIVACY NOTICES

The GDPR requires controllers to provide individuals with detailed information with respect to their personal data (which is usually provided through a privacy notice) in concise, easy to understand, and clear language. The information that must be disclosed includes the identity of the controller, how the data will be used, the legal basis justifying the processing of the data, data retention periods, any transfer of the data outside the European Economic Area (the EEA, comprising the EU Member States, Norway, Iceland, and Lichtenstein), and investors' rights, including the right to lodge a complaint with the Data Protection Authority.

Tip: Review employee notices, tenants notices, investor notices and website privacy policies, and update them to ensure GDPR compliance. If your website uses cookies and similar technologies, you should also be aware of the additional notice and consent requirements under electronic privacy (e-Privacy) regulations.

4. REVIEWING THE LEGAL BASES FOR DATA PROCESSING

The GDPR requires that controllers have a "legal basis" to process personal data. Examples of a legal basis include individual consent, the need to perform a contract with the data subject or to comply with legal obligations, or the "legitimate interest" of the controller or a third party.

A number of typical data processing activities carried out by CRE businesses are likely to be justified by the need to perform obligations under the relevant agreement with the data subject, or to comply with EU legal obligations, while others (for example, complying with a non-EU legal obligations or use of asset and property managers) are justifiable as legitimate interests. Any other processing activities that cannot be justified under one of these legal bases, for example, marketing, will usually need to be based on "consent" from individuals.

The GDPR significantly tightens the rules for obtaining consent. Consent must be an affirmative indication by individuals that they agree to their personal data being processed for clearly identified and specific purposes. Silence, inactivity, or pre-ticked boxes are invalid. For certain processing activities (for example, transfer of data outside the EEA), consent must be "explicit," i.e., affirmed in a clear statement rather than by any other positive action. Moreover, the request for consent must be presented in a manner that is clearly distinguishable from other terms (it should not be "buried" in privacy policies, or terms and conditions). Individuals must be able to withdraw consent at any time and in an easy way. CRE businesses will need to specifically reconsider the way they phrase and present consent requests or forms to ensure compliance with the GDPR's enhanced requirements.

Tip: Consider the various types of data processing you carry out, and identify and document the legal basis you are relying on for each purpose for which you are processing data. Where consent has previously been relied upon to justify processing activities, assess whether those existing consents meet the GDPR's elevated requirements. If they do not, you should consider taking action to obtain fresh GDPR-compliant consent from individuals, and review standard-form language in the subscription forms and other documents you are currently using (unless another legal basis for processing can be established).

5. IMPLEMENTING DATA TRANSFER MECHANISMS

The GDPR prohibits the transfer of personal data to countries outside the EEA that are not considered to offer adequate privacy protections. Ongoing routine transfers of personal data outside the EEA must be legitimized by a valid transfer mechanism including the EU-U.S. (or, if applicable, the Swiss-U.S.) Privacy Shield or Standard Contractual Clauses (SCCs). Data transfer restrictions can pose a significant challenge to U.S. companies, as the valid transfer mechanism contemplated by the GDPR may not be readily available. For example, the EU-U.S. and Swiss-U.S. Privacy Shield frameworks are only available to companies that are subject to the jurisdiction of the U.S. Federal Trade Commission or the Department of Transportation. SCCs require a business ("data exporter") based in the EEA and cannot be entered into with data subjects.

Transfers may still be legitimized on the basis of certain derogations, such as consent from individuals, or where it is necessary to perform a contract. Approved codes of conduct and certification mechanisms may also be used in the future to provide further and alternative authorization for data transfers.

Tip: Consider the extent to which you transfer personal data outside the EEA – both intragroup and to service providers – and review the mechanisms you rely on to accomplish such transfers to ensure they meet the GDPR requirements. If your data export strategy is built around consent from individuals, assess whether existing consents meet the GDPR's elevated requirements and evaluate whether consent is a practical solution for your data processing activities, especially given that consent can be withdrawn by individuals at any time and, being a derogation to the requirement on controllers to implement appropriate safeguards, is subject to a restrictive interpretation.

6. REVIEWING DATA PROCESSING AGREEMENTS

Controllers must ensure that data processing terms are in place with all data processors that process personal data on their behalf (for example, property managers, payroll processing, cloud service providers). The GDPR is prescriptive about the content of such terms. Mandatory content includes specific information on the data processing, restrictions on sub-processing, cooperation with the controller in fulfilling the GDPR's obligations, and controller's audit rights.

Most multi-national technology service providers are well prepared for the GDPR and have template data processing agreements ready to roll out to their customers. However, many controllers in the CRE industry are not accustomed to such requirements, especially with respect to their IT systems and back-office administrative functions. There can be significant negotiation around the data processor's rights and obligations, especially in relation to liability, as the industry seeks to navigate some norms in this new environment.

Processors are, in turn, required to contractually flow down the obligations in the data processing agreement to their sub-processors. This requirement can pose challenges when the chosen sub-processors are able to leverage their market power and impede the GDPR's construct of empowering the controller to control the data processing throughout the processing chain.

Tip: Review processing terms contained in property management agreements, and other contracts with service providers to ensure that they contain the terms prescribed by the GDPR.

Before engaging a data processor, assess the processor's ability to ensure compliance with the GDPR's increased obligations. As under the current framework, controllers are ultimately responsible for compliance with data protection principles and can be liable for the failings of their processors in some circumstances.

7. RECORD-KEEPING

The GDPR requires controllers and processors to keep detailed records of data processing. Records must be provided to data protection authorities upon request. The GDPR is prescriptive on this requirement and specifies the minimum information to be included in these records.

Some EU authorities have announced that they will launch investigations and ask randomly selected businesses to provide copy of their processing records. Although such announcements appear to target only businesses with an EU establishment for the time being, all companies should be prepared to review and hand over the records upon requests (including, for non-EU based businesses, through their EU based representative (see below)).

Tip: Develop and maintain records of processing activities, and establish procedures for regularly updating your records.

8. PREPARING DATA BREACH PROCEDURES

The data breach notification requirement is a significant new feature of the GDPR, although U.S. businesses will be accustomed to data breach notification obligations imposed by state laws. Notably, the GDPR requires controllers to notify authorities of certain "personal data breaches" within 72 hours of becoming aware of the breach, unless they can show the risk to individuals is unlikely. Likewise, affected individuals must be notified without "undue delay" if the breach is likely to result in a "high risk" to their rights and freedoms. Processors are required to notify controllers without undue delay after becoming aware of a breach.

Not all security incidents are necessarily personal data breaches. Companies inevitably experience security breaches from time to time, but whether an incident is a reportable breach requires a careful risk assessment. Moreover, businesses operating in multiple jurisdictions must also consider the interplay of the GDPR's breach notification obligations with mandatory breach notification obligations outside the EU (e.g., the U.S., Mexico and Australia). Relevant differences should be accounted for in incident response plans and policies and employees should receive regular training on such differences.

Tip: Assess your internal policies and processes to ensure that appropriate procedures are in place to detect, investigate, report, and document data breaches and to manage the fallout from such reporting. Ensure that your contracts with data processors incorporate terms requiring such processors to notify you of data breaches in time to meet the GDPR's notification timeframes.

9. REVIEWING PROCEDURES AND POLICIES TO COMPLY WITH INDIVIDUALS' RIGHTS

The GDPR significantly enhances the rights of individuals. Tenants and employees have augmented rights relating to their data, including to access, to require erasure (the "right to be forgotten") and to restrict "automated decision-making" (e.g., automatic refusal of an online

credit application; e-recruiting practices without any human intervention). It also introduces a new right to "data portability" (the right to receive one's personal data electronically and in a commonly used format, and to move such data to another controller). The GDPR imposes tight timeframes to address individuals' requests – controllers will need to provide information on actions taken on a request within one month of receipt (subject to extensions under certain circumstances).

Tip: Review your internal processes, staff training and IT systems, and make any necessary changes to accommodate these new individuals' rights.

10. OTHER REQUIREMENTS

Data Protection Officer

The GDPR requires businesses to appoint a Data Protection Officer ("DPO") in specified circumstances, most notably where an entity's key operations ("core activities") consist of (1) processing of personal data about criminal convictions and offenses, or of sensitive data or (2) regular and systematic monitoring of data subjects, in either case on a large scale (having regard to factors such as number of individuals involved and geographical reach). CRE businesses conducting surveillance at their properties would need to assess the requirements carefully.

Tip: Assess whether any of your core activities would require you to appoint a DPO and document this internal analysis. If you have already hired a DPO, you should review the job functions of the position and compare them to the GDPR's requirements (e.g., expertise and independence), and adapt the functions as warranted.

Privacy by Design and by Default

Controllers must implement appropriate security measures in order to integrate data protection principles into data processing activities ("Privacy by Design"), such as pseudonymization – the separation of data from direct identifiers so that linkage to an identity is not possible without additional information that is held separately. They must also ensure that processes in place are such that, by default, only personal data that are necessary for each specific purpose are processed ("Privacy by Default").

Tip: Ensure that your technology infrastructure, information systems, privacy programs, and processes address the GDPR's Privacy by Design and Privacy by Default requirements. This will involve an examination of the life cycle of personal data that are being handled against these requirements of the GDPR.

EU Representative

Non-EU CRE group that are subject to the GDPR will, in most cases, be required to appoint an EU-based representative in connection with their GDPR obligations. The role of the EU representative is to act on behalf of the party appointing it with respect to that party's obligations under the GDPR. Investors and the authorities are entitled to "address" the EU representative, without affecting their rights against the controller or processor. Authorities may bring enforcement proceedings directly against the EU representative instead of the controller or processor.

Tip: A number of organizations offer to fulfil the role of EU representative. Unsurprisingly, they inevitably seek robust indemnity protection for fines, claims, and losses arising in

connection with the role. Companies should investigate the available options and appoint an appropriate representative, giving careful consideration to the mandate granted to the representative.

Identifying the Lead Data Protection Authority

Businesses with multiple establishments in the EU (or whose sole EU establishment carries out data processing activities that substantially affect individuals in multiple Member States) may now benefit from a new ‘‘one-stop shop’’ approach to enforcement. Under this approach, the Data Protection Authority of the entity’s “main” establishment acts as the “lead” Data Protection Authority to coordinate investigations and enforcement actions concerning such entity’s compliance with the GDPR, thus avoiding having to deal with multiple Data Protection Authorities.

Tip: Identify where your “main establishment” is and who your lead Data Protection Authority will be, and document the internal analysis carried out in this respect in order to be able to provide the Data Protection Authority with evidence of your main establishment.

CONCLUSIONS

Notwithstanding the GDPR is now enforceable, many CRE businesses are still actively working toward compliance. Authorities have been working proactively with business to encourage compliance but recent investigations and enforcement actions reflect a clear message as to their expectations.

There is an increasing focus on the intersection of technology, privacy and ethics amongst regulators. For those in the CRE sector embracing PropTech and its multitude of exciting possibilities, they will need to build a data protection culture within their respective organizations, consider data protection principles in new technologies and implement robust policies and procedures to demonstrate data protection compliance.

About the Authors

Brenda Sharton is the Chair of Goodwin’s Privacy and Cybersecurity practice. Karen Neuman and Gretchen Scott are partners, and Federica De Santis is an associate, in the firm’s Privacy and Cybersecurity practice. Minta Kay is the Chair of Goodwin’s Real Estate Industry practice and the Co-Chair of the firm’s PropTech Initiative.