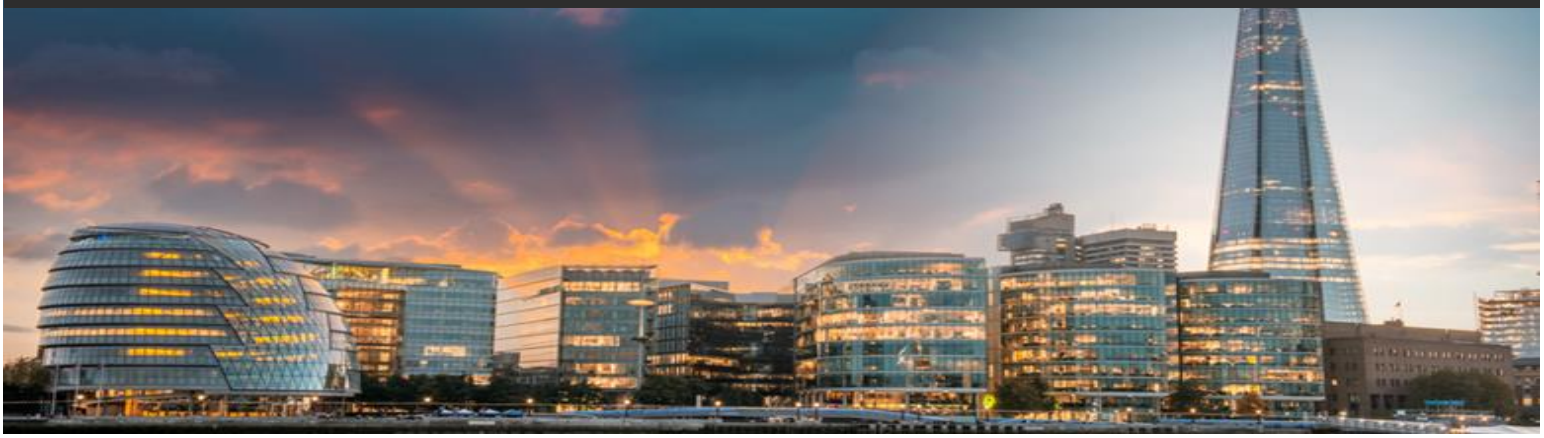
GT GreenbergTraurig | 50TH ANNIVERSARY

Alert | Franchise & Distribution/ Cybersecurity, Privacy & Crisis Management



November 2017

EU General Data Protection Regulation: What Impact for Franchise Businesses?

One of the most important assets that a franchise business has is its customer data. For a franchise business, data protection/data privacy regulation should be a key compliance issue. This is particularly the case in Europe, which has had comprehensive data protection laws for many years, and is reforming those laws into a legislative framework that will feature some of the strictest and furthest-reaching data protection obligations in the world.

Following several years of legislative debate and amendment, the EU General Data Protection Regulation (GDPR) will come into force in the European Union on 25 May 2018.

The GDPR is not just an update of a 20-year-old Directive that was designed at the dawn of the internet era, and based on privacy principles published by the Organisation for Economic Co-operation and Development (OECD) in the early 1980s. The approval of the GDPR is a significant development in the shaping of the law of privacy and data protection in the European Union (EU) as a cohesive, homogenous whole, where one single law becomes the primary vehicle to govern the activities of very diverse countries in a particular domain.

This GT Alert focuses on some of the main GDPR obligations faced by franchise businesses, including those whose principal business establishment is located outside the EU and the European Economic Area (EEA).

Whom does the GDPR target?

The GDPR applies to "data controllers" and "data processors". A "data controller" is a person or entity that determines the purposes, conditions and means of processing personal data. A "data processor" is a person or entity that processes personal data on behalf of a data controller.

Franchisees will be affected as data controllers because they (amongst other things) collect, store, analyse and share data relating to individuals (mainly, their customers and employees). Franchisors can also be affected as data controllers even if based outside of Europe to the extent a franchisor collects and stores data relating to their EU franchisees' customers, such as for customer loyalty programs. In addition, to the extent franchisees are collecting data on behalf of the franchisor, the franchisees will be affected as a data processor. As such, all franchisors and franchisees with operations in Europe will need to consider how the new law applies to them, and how to become compliant.

Based outside the EU? The new law can still apply to you.

The GDPR may apply to franchise businesses even if they are based outside Europe. If your franchise does any business in Europe or collects any personal data relating to European residents, the GDPR is likely to apply to your company, wherever it is located. Indeed, the GDPR will apply not only to all franchise businesses that are established in the EU/EEA and collect or process personal data in the EU/EEA, but also to franchisors established outside the EU or EEA if they are collecting or processing personal data from European residents.

The GDPR applies to the processing of personal data in the context of the activities of an establishment of a data controller or data processor in the EU/EEA, regardless of whether that processing takes place in the EU/EEA or not. It will also apply to the processing of personal data of individuals who reside in the EU/EEA when the processing is conducted by a data controller or data processor that is not established in the EU/EEA, if such processing relates to: (i) the offering of goods or services in the EU/EEA, whether payment is required or not; or (ii) the monitoring of such individual's behaviour, to the extent that such behaviour takes place within the EU/EEA.

Single Rule...Almost all the Time

The new rule is framed as a "Regulation" rather than a Directive, which means that it is directly applicable in each of the EU Member States and does not need to be transposed into each country's legal framework. The existing EU/EEA data protection framework is based instead on a series of Directives, the main one being Directive 95/46/EC, which are only foundational documents with limited direct application and direct the Member States to enact laws that are consistent with the provision of the relevant Directive. As such, the implementation of the 1995 Directive resulted in the creation of national data protection laws that had some resemblance but differed substantially from each other.

The GDPR is intended to bring uniformity across the EU/EEA. However, it contains numerous provisions that give leeway to each Member State. Franchisors and franchisees, alike, must therefore be careful not to be fooled by the appearance of a single rule, and should instead consider the GDPR as a general rule in addition to the numerous national exceptions or supplements that are likely to be created.

No More Notification…but More Paperwork

Currently, franchise businesses that do business in multiple EU/EEA member states complain about the significant administrative burden and related costs that were associated with compliance with the "notification" requirements under the Directive. Registration requirements and procedures differ from country to country.

The GDPR puts an end to the notification requirement. However, it defines a new regime of accountability, where companies will have to prepare and maintain numerous documents and reports to protect their practices and policies with respect to the handling of personal information, as well as a written information plan to carefully document their information systems and their personal data processing.

Privacy Notices

Franchise businesses should review their privacy policies and notices to ensure that they are compliant with the requirements set down by the GDPR.

The GDPR enhances the obligations on data controllers to provide information to data subjects about how their personal data will be processed. Under the GDPR, a data controller must provide clear information to data subjects about its processing of their data, unless the data subject already has this information. This obligation exists in the current Directive, but the GDPR strengthens the requirement.

Consent

Many franchise businesses use customer consent as a basis for processing their personal data. The GDPR will introduce stiffer rules around the "quality" of consent that must be obtained from customers.

Where processing of personal data is based on consent, the data controller must be able to demonstrate that such consent was given. Under the GDPR, an individual's consent must be given freely, specific, informed and unambiguous. If an individual gives consent in a written declaration that concerns other matters, the request for consent must be presented in a manner that is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language. Otherwise, it will not be binding. Thus "implied consent" appears to be practically ruled out.

Furthermore, the GDPR will require data controllers to allow individuals to withdraw consent easily and at any time. The GDPR also provides for rules to assess whether consent actually was given freely. For example, consideration will be given to whether the performance of a contract was made conditional on the consent without the relevant data being necessary for such performance.

Without consent, the processing will be deemed lawful only in specific circumstances where the data is processed on a legitimate basis under the GDPR or another law, for example if the data is processed as a necessity for compliance with legal obligations to which the data controller is subject, or the necessity for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject before entering into a contract.

Privacy by Design and Default

Franchise businesses will have to place data protection compliance close to the heart of new business practices or systems they develop. The GDPR sets out a number of new "data governance" principles which will create new operational obligations and costs for many public and private sector organisations.

These include the formal introduction of "Privacy by Design" and the use (where appropriate) of "Privacy Impact Assessments".

Under the "Privacy by Design" principle, franchise businesses will be required to implement technical and organisational measures to show they have considered and integrated data compliance measures into their data processing activities.

The GDPR will also require franchise businesses that are data controllers to conduct Privacy Impact Assessments (PIAs) before they undertake processing of personal data which presents a high risk to the data subjects' rights and freedoms.

Using Data Processors

Franchises that use third parties to process their personal data (be it customer data or otherwise) will need to review and (re)negotiate their data processing agreements with those third parties.

The GDPR imposes a higher duty of care on data controllers in selecting the organisations that process personal data on their behalf than under the predecessor Directive.

The GDPR requires that, where a data controller uses a data processor to process personal data on its behalf, it must enter into a written contract with that processor which must include certain information and obligations. This also applies further down the processing chain, *e.g.*, where a data processor uses a sub-processor.

Personal Data Breach Notification

For the first time, franchise businesses will be required to investigate and report personal data breaches that they experience.

The GDPR implements rules regarding the response to a breach of security. A "personal data breach" is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or processed".

The notification of a personal data breach will occur in two successive phases.

Where a franchise business is a data controller, it will be required to notify the competent supervisory authority of a breach "without undue delay" and, if feasible, no later than 72 hours, unless it is unlikely that the breach will result "in a risk to the rights and freedoms of individuals". If the breach is not notified within 72 hours, the subsequent notification must indicate the reasons for the delay. When a breach affects a franchise business that is a data processor on behalf of a data controller, it must notify the data controller "without undue delay" after becoming aware of the breach.

If the breach is likely to result in a "high risk to the rights and freedoms of individuals", the data controller also will be required to inform the data subjects without undue delay of the occurrence of the breach unless an exception applies. If a data controller fails to notify the affected individuals, the supervisory body may require the data controller to do so, or may decide that an exception applies.

The GDPR does not define "risk" and "high risk" or provide any guidelines about the difference between the two concepts.

Do we need to appoint a Data Protection Officer?

Franchise businesses will need to consider whether to appoint a data protection officer.

Certain categories of data controllers or data processors will have to appoint a data protection officer. This requirement will apply to all organisations whose core activity consists of the following when they are conducted on a large scale:

- The regular and systematic monitoring of data subjects;
- The processing of special categories of personal data; or
- The processing of data relating to criminal convictions and offences.

Groups of companies will be able to appoint a single data protection officer if that person is easily accessible from each establishment.

What are the fines for non-compliance?

The GDPR will introduce a new regime of fines and penalties which are considerably greater than exist under the present legislation.

Fines for violations of the basic GDPR principles for data processing (including but not limited to inability to demonstrate that consent was obtained) as well as non-compliance with certain orders of the competent advisory authority, can be up to the greater of Euro 20 million or 4 percent of the total worldwide annual turnover of the company for the preceding financial year. For other violations, fines can be up to the greater of Euro 10 million or 2 per cent of such turnover.

In addition, the GDPR allows EU Member States to enact rules for other penalties that would be applicable to infringements of the GDPR that are not subject to the pre-defined administrative fines.

Will Brexit affect the GDPR?

In spite of Brexit, franchise businesses operating in the UK should still pursue a GDPR compliance programme. Brexit will have minimal impact on the GDPR's applicability to the UK.

The UK government has confirmed that the UK will implement the GDPR into its own national law, regardless of the effects of Brexit. In doing so, the UK government's intention is to ensure that the country's data protection framework is *"suitable for our new digital age, allowing citizens to better control their data"*.

To this end, the UK government recently published the UK Data Protection Bill, which is intended to incorporate the GDPR (with permitted changes) into UK law and provide continuity both during and after the Brexit process.

Concluding Comments

Franchise businesses should start preparing now (if they have not already done so) to ensure that their European data processing practices are in good shape to meet the demands of the new legislation.

Authors

This GT Alert was prepared by **Alan R. Greenfield** and **Luke Dixon**. Questions about this information can be directed to:

- Alan R. Greenfield | +1 312.456.6586 | greenfieldalan@gtlaw.com
- Luke Dixon | +44 (0) 203.349.8756 | dixonl@gtlaw.com
- Or your Greenberg Traurig attorney