Prepared for the PRCA by Lewis SIlkin

LEWIS SILKIN

PR Agencies
Getting data protection ready!

PRCA
The Power of Communication

The General Data Protection Regulation ("GDPR"), takes effect from 25 May 2018, and brings about important privacy changes that will impact most businesses, including those which deal with personal data for and on behalf of their clients and suppliers. The GDPR is lengthy, complex and prescriptive - this gives rise to new challenges for PR agencies which need careful thought, largely to minimise risk and additional cost.

In this note, we seek to give PRCA members a flavour of the key changes arising from GDPR.

We focus on PR agencies' obligations as a '*data processor*'. Of course, in several instances, a PR agency may also be a 'data controller' acting on its own or a 'joint data controller' or 'data controller in common' with a third party, but that is not the focus here.

It is likely that clients will look to share the burden of their GDPR obligations with their PR agency. We therefore look at the key GDPR challenges facing these processors in two parts: (i) direct GDPR obligations, and (ii) indirect GDPR obligations likely to arise in the context of work for their clients.

Although GDPR is a European Regulation, its far reaching territorial scope means that even businesses located outside of the European Economic Area (EEA) will also be caught if they are processing personal data of EU citizens.

Direct obligations on processors

Increased cost and exposure

Under GDPR, data processors will now, for the first time, become directly accountable to the Information Commissioner's Office (ICO) or other regulators for compliance with certain obligations. These include obligations on processors to:

(a) have in place adequate security measures;

(b) delete or return personal data on contract termination

(c) keep comprehensive records of data processing activities;

(d) co-operate with, and provide access rights to systems, premises and records, to regulators and data controllers alike; and

(e) ensure that their obligations are 'flowed down' onto sub-processors (i.e. sub-contractors and some suppliers) and, in practice, take on responsibility for sub-processors.

Any consumer (or other person) who suffers damage as a result of breach of GDPR has a right of compensation from the controller or processor for breach of their respective obligations. However, a processor can also be liable where it has acted outside or contrary to the lawful instructions of the controller.

GDPR makes data processors directly liable for fines for breach of their obligations up to the greater of 2% of worldwide turnover and €10 million. In some cases, those numbers increase to 4% and €20 million respectively, for example where a processor makes unauthorised data transfers outside of the EEA or where it acts outside the lawful authority of the controller.

We'd be surprised if the ICO flexes the full might of its new muscles in 2018, but the fining ability nonetheless presents a significant new exposure. Agencies should be taking steps to see how their exposure can be minimised. One key step is to build or adapt solutions that *minimise* the amount of personal data being processed and/or to encrypt data and to put corresponding responsibilities on any third parties involved with the data processing. Other risk reduction techniques might include seeking to reallocate contractual risk to clients, given that the agency, as a processor, will be directly accountable to the regulator. This could be done by widening exclusions of liability and ensuring back-to-back agreements with suppliers and sub-contractors are present and correct. Agencies should also consider appropriate types of insurance, including professional indemnity, business continuity and data breach insurance.

Sub-processors

As data processors, PR agencies will be responsible for obtaining the data controller's prior written consent (whether specific or general consent) if they wish to delegate any processing activities. They will also be responsible for the actions, omissions and failures of their sub-processors. Compliance is not straightforward, as it might not be clear who all the sub-processors will be at the outset of a project or relationship. To avoid having to get specific consent each time they wish to appoint a sub-processor, agencies should consider getting general authorisation up front. If an agency wishes to rely on obtaining general consent, it will be required to notify its clients each time it appoints a sub-processor and provide them with opportunity to object. Agencies should consider including parameters around this right of objection and consider their options where a client objects. One option could be to include a right of termination for the agency where a client objects; this should act as a deterrent and help to avoid any potential breach of contract claim for not being able to perform the services or deliver the

solution as agreed.

Heightened focus on security

Data security is now more than ever a concern for consumers, customers and governments, so it is no surprise that one of the main obligations on data processors is to ensure adequate security.

Under GDPR, processors must implement 'appropriate technical and organisational measures' to ensure personal data is kept secure (taking into account factors such as state of the art and cost). GDPR is more prescriptive than the current Data Protection Act (DPA) and states that these measures may include (a) encrypting (and 'pseudonymising') personal data; (b) having the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services; (c) having the ability to restore availability of, and access to, personal data in a timely manner in the event of a physical or technical incident; and (d) a process for regularly testing, assessing and evaluating the effectiveness of all these measures, to ensure data security. This is onerous stuff, which needs to be factored into pricing models.

Appointment of a DPO

PR Agencies whose core activities consist of processing operations that require regular and systematic monitoring of data subjects on a large scale will now have to appoint a data protection officer (DPO). "Core activities" won't include support functions such as HR and payroll, but could include data collected as an inextricable part of the pursuit of business goals. For example;

> The DPO must be a person with expert knowledge of data protection law and practices, whose job is to monitor internal compliance with the GDPR. As the DPO must not have a conflict of interest in conducting his/her role as a DPO, a CEO, FD, IT Director or Marketing Director can't hold the role. Note that a DPO cannot be penalised or dismissed for performing their duties.

The guidance states that "regular and systematic monitoring" will include internet tracking and profiling for the purpose of behavioural advertising, providing telecoms services, credit and risk assessment, location tracking, loyalty schemes and the operation of smart appliances. What is meant by "large scale" hasn't been defined, but factors to consider include the number of individuals monitored, the geographic extent and permanency of the personal data collected and the volume or range of data processed.

Record keeping and audit requirements

Controllers will no longer be required to notify the relevant data protection authority that they are a data controller. However, controllers **and** processors are each required to maintain detailed records regarding their respective data processing activities and to be able to evidence compliance with the GDPR. The new requirements are likely to be more onerous iwn most cases and PR agencies need to ascertain how they will comply, which may require advance discussions with clients, especially where client requirements change or are made with little notice. Data processors may also wish to consider whether to put in place self-certification audit processes to meet the new audit requirements imposed on both controllers and processors under GDPR.

Indirect obligations on processors arising through vendor management

Privacy by design

A key over-riding principle of GDPR is the concept of 'privacy by design'.

This means that businesses need to put in place processes and procedures to ensure **privacy by design** and **by default**. PR agencies must have data privacy at the forefront of their minds when engaging with any briefs or work which involve processing personal data. For example, think about ways in which the volume of personal data can be minimised, including through anonymisation and pseudonymisation techniques or simply being more focused about the data that is really needed. Also, consider how the responsibility for this filtering process can be passed on to the client. Speak to clients about any privacy impact assessments they may have in the pipeline, as these will inevitably have an impact on the agency's costs, obligations and timeframes.

New data subject rights

GDPR codifies a number of existing data subject rights and introduces some new rights, all of which PR agencies need to be alive to. These rights are important and include a right to object, right to be forgotten, right of rectification and right of access. Although some of these rights exist now, data controllers will be required to ensure that all data subjects are aware of their rights which, in turn, mean that the likelihood of them being exercised is greater, and will impact the cost of compliance for data processors.

End consumers and other data subjects also benefit from a new data portability right which gives them the right, in certain circumstances, to request that the data controller provides them, in machine readable format, with all personal data provided to the data controller by the data subject. Many data controllers will contractually be 'backing-off' this obligation onto their data processors. Agencies should consider the impact of these changes, and potential scope and costs.

Data breach notification

GDPR introduces mandatory data breach notifications to the regulator within **72 hours** and in more serious cases requires data subjects to be notified.

Although the primary obligation to notify the regulator (and data subject) rests with the data controller, data processors will be required to notify the data controller of data breaches without undue delay. Staff training should, in particular, be implemented to ensure this can be achieved.

All providers, especially those operating across the EU, should have joined-up and well-rehearsed data security and breach procedures in place which can enable breach notifications to be made quickly, including having appropriate external support in place, such as PR and DR resources.

Closing thoughts and next steps

While well intentioned, the GDPR is too prescriptive for 21st century PR agencies, which vary significantly in size and remit, but it's here to stay. Brexit or no Brexit. Taking the time now to adjust offerings, systems, processes and (importantly) contracts, will help PR agencies not only to manage their own risk and cost base, but also to provide reassurance to clients and improve the attractiveness of their offerings. All this should, of course, help to improve (or at least reduce the impact on) the bottom line.

For further information on this subject please contact:

Bryony Long
Senior Associate, Data & Privacy

+44 (0) 20 7074 8435
bryony.long@lewissilkin.com

James Gill
Partner, Data & Privacy

+44 (0) 20 7074 8217
james.gill@lewissilkin.com

Geraint Lloyd-Taylor
Legal Director, Advertising & Marketing

+44 (0) 20 7074 8450
geraint.lloyd-taylor@lewissilkin.com

LEWIS SILKIN

5 Chancery Lane – Clifford's Inn
London EC4A 1BL
DX 182 Chancery Lane
T +44 (0)20 7074 8000 | **F** +44 (0)20 7864 1200
www.lewissilkin.com