EU update

Kit Burden1,*

DLA Piper UK LLP, United Kingdom

ABSTRACT

This is the latest edition of the DLA Piper column on developments in EU law relating to IP, IT and telecommunications. This news article summarises recent developments that are considered important for practitioners, students and academics in a wide range of information technology, e-commerce, telecommunications and intellectual property areas. It cannot be exhaustive but intends to address the important points. This is a hard copy reference guide, but links to outside web sites are included where possible. No responsibility is assumed for the accuracy of information contained in these links.

© 2017 DLA Piper UK LLP. Published by Elsevier Ltd. All rights reserved.

Keywords:
EU law
Intellectual property
Information technology law
Telecommunications law

1. Top five takeaways on how to get ready for the European Privacy Regulation

Giulio Coraggio, Partner, DLA Piper Italy

1.1. GDPR compliant privacy information notice and consents cannot wait

As provided by the recent guidelines of the Italian privacy authority, data protection regulators expect that on the 25th of May 2018 companies already have in place a privacy information notice compliant with the European General Data Protection Regulation and have obtained the required consents.

This step not only requires to put in place a “transitional” privacy information notice, but also to implement technical changes in order to, among others, manage

- the deletion of personal data on the expiry of the storage period,
- the data portability right and
- the new consents to be requested.

1.2. A data governance system is a “must-have”

The GDPR requires to have a full control of processed data. This can be achieved through the combination of organisational measures and technical tools. A data governance system able to map at any time data in information systems is necessary as otherwise for instance

- the record of processing activities cannot be up-to-date,
- the storage period of each category of data cannot be monitored and
- the exercise of the data portability right risks to be lead to the loss of valuable know-how and assets.

1.3. The data portability right requires an ad hoc procedure and technical functionalities

The data portability right is definitely the most interesting change introduced by the GDPR. Its management requires

- not only to decide how data shall be ported to a third party, but also
- tools to identify which data shall be ported,

* DLA Piper UK LLP, 3 Noble Street, London, EC2V 7EE, United Kingdom.
E-mail address: kit.burden@dlapiper.com.

1 For further information see: http://www.dlapiper.com/
http://dx.doi.org/10.1016/j.clsr.2017.08.005
0267-3649/© 2017 DLA Piper UK LLP. Published by Elsevier Ltd. All rights reserved.
organisational measures to obtain the approval by the data subject and
when data is received from a third party solutions to assess which ported data can be retained.

1.4. Internal technical and organisational checks need to reach a higher level

In a number of companies personal data of customers is accessible to a large number of employees with no major technical restriction to the usage of such data and internal organisational checks on data processing activities are just formalities often ignored.

With the GDPR, the accountability principle requires a major change to privacy compliance which implies

- a more detailed review of the profiles of access to personal data;
- the implementation of technical solutions to identify potential misuses of personal data; and
- a reorganisation of the individuals appointed internally to monitor data protection compliance. The matter cannot be fully delegated to the DPO who also needs to be in a position of independence to be able to perform his activity in compliance with the strict requirements of the GDPR.

1.5. Checks need to be extended to external suppliers

It is interesting that also very large companies do not have a list of all their external suppliers and the checks performed on them are either only security related or if privacy checks are run these are merely formal.

On the contrary, internal procedures shall be put in place in order to

- create a list of all the external suppliers and ensure that they all entered into a GDPR compliant data processing agreement;
- run checks on external supplies by means of a checklist at the time of the execution of the contract and during its life;
- perform random audits on them and
- depending on the specific circumstances of the case, perform also privacy specific trainings to their benefit.

1.6. Practical impacts of GDPR on the employment relationship

1.6.1. Data subject access requests

Under the GDPR, employees will have the right to much more detailed, transparent and accessible information about the processing of their data. Data subject access requests will be easier for employees. In most cases employers will not be able to charge for complying with a request and normally will have just a month to comply, rather than the current 40 days. The removal of the £10 subject access fee is a significant change from the existing rules under the Data Protection Act (DPA).

Where requests are complex a two month extension is possible, giving a total of three months to comply. Where requests are manifestly unfounded or excessive, in particular because they are repetitive, employers can either charge a reasonable fee (not capped) taking into account the administrative costs of providing the information, or refuse to respond.

Guidance will hopefully give an indication in due course of what sorts of requests could be viewed as complex, unfounded or excessive. However, the ICO is very unlikely to consider a request from an employee as complex, unfounded or excessive, even if they are asking for all their data, unless they have made a previous request recently. The ICO will expect employers to keep information in a manner which means they can locate and supply information within the initial month.

Where an employer intends to delay the response or refuses to respond to a request, the employer must write promptly to the individual within the month explaining why the request is refused or delayed. The employer must also inform them of their right to complain to the supervisory authority and to a judicial remedy.

The DPA contains various exemptions to the duty to disclose such as in relation to legal privilege but at present, the GDPR contains no such exemptions which an employer can rely on to avoid provision of the employee’s personal data. It may be that, in the UK at least, the doctrine of privilege will ‘trump’ data protection rights, but that remains to be tested.

Employers need to update procedures and plan how to handle requests within the new timescales. The GDPR introduces a new best practice recommendation that, where possible, organisations should be able to provide remote access to a secure self-service system which would provide the individual with direct access to his or her information. This will not be appropriate for all organisations, but there are some sectors where this may work well. In any event the ICO will expect employers to keep employee personal data in a manner which means that requests for access can be responded to promptly.

What this means in practice is that employers will need sophisticated policies and IT systems to manage DSARs within reasonable timeframes. In order to prepare for compliance, employers should take steps now to:

- Update procedures and plan how to handle SARs and provide any additional information within the new timescales;
- Develop template response letters to ensure that all elements of a response to a SAR under the GDPR are complied with;
- Assess the organisation’s ability to isolate data pertaining to a specific individual quickly and to provide data in compliance with the GDPR’s format obligations;
- Ensure that employees are trained to recognise and respond quickly and appropriately to SARs.
- Consider putting a ‘data subject access portal’ in place allowing an individual to access their information easily online.

1.6.2. Automated processing and profiling

Employees have a right under the GDPR to not be subject to a decision made solely by automated processing where that decision significantly affects them. This includes decisions based on profiling (any form of automated processing to evaluate certain personal aspects of individuals, in particular to analyse
دریافت فوری متن کامل مقاله

امکان دانلود نسخه تمام متن مقالات انگلیسی
امکان دانلود نسخه ترجمه شده مقالات
پذیرش سفارش ترجمه تخصصی
امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
امکان دانلود رایگان ۲ صفحه اول هر مقاله
امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
دانلود فوری مقاله پس از پرداخت آنلاین
پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات