MILLS & REEVE

briefing

April 2018

GDPR: cross-border perspectives

With the implementation of the EU-wide General Data Protection Regulation imminent, we look at what HR departments are doing to get ready in four EU jurisdictions: France, Germany, the Netherlands and the UK.

Overview

When is the Regulation coming into effect?

The General Data Protection Regulation will take direct effect across the entire EU on 25 May 2018. Unlike the current data protection regime, deriving from 1995 Data Protection Directive, specific legislation by individual member states is not required in order to give it effect in each individual jurisdiction.

However many member states, including all four countries featured in this briefing, will be legislating so that they can take advantage of permitted derogations or strengthen domestic protection where the GDPR gives them this flexibility.

What is changing?

Many of the key data protection principles remain the same, but it has been felt necessary to increase the level of protection for individuals and strengthen penalties for non-compliance in the light of the vastly greater amounts of personal data now being processed in the social media age.

Significant changes from the current regime EU regime include:

- A greater emphasis on transparency by data controllers.
- Tightening the restrictions on processing sensitive personal data (now to be called “special categories of personal data”).
- A strengthened “right to be forgotten”.
- A new right to “data portability”.
- Wider obligations to report data protection breaches.
- Abolition of the subject access fee in most circumstances plus reduced time for compliance.
- Scope for imposing much greater fines for non-compliance – in some cases up to 20 million Euros or 4 per cent of worldwide turnover.

Article 88 gives member states a degree of flexibility in the context of employment. It allows them to make provision “for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees’ personal data”.

France

How is the GDPR implemented?

Even though GDPR will be directly applicable in France as of 25 May 2018, France is currently discussing a bill to modify Act n°78-17 of 6 January 1978 on information technology, data files and civil liberties which regulates data processing in France.

What specific rules will be adopted in relation to employee data?

Act n°78-17 already provided for limited derogations such as processing for which "the data subject has given their express consent, except in cases where the law stipulates that the prohibition may not be lifted by the consent of the data subject".

The bill is adding a few derogations to the list including, in relation to employee data, "processing of biometric data which are strictly necessary to control access to working places, equipment and software used by employees to carry out their missions" (bill article 7 modifying art 8 of Act n°78-17).

What do HR departments see as the main challenges?

Obligation to open a register with a list of existing data processing: Applicable to companies of 250 employees and above and companies of fewer than 250 employees when such processing may create a risk for individual rights and liberties. So basically all companies are at risk and it requires that they make an audit of all existing data processing (recruitment process, active employees, former employees, payroll, driving licenses, video monitoring, access cards, trainings, family situation, absences, etc.)

Obligation to appoint a Data Privacy Officer (DPO): Today, companies may decide to appoint a DPO ("CIL" in French). With the GDPR, private companies will have the obligation to appoint a DPO if their specific activity regularly and systematically consists in processing a huge amount of personal data (for example, interim agencies or head-hunting companies) or when the data processed are sensitive (race, religion, origin, political orientation, or criminal records, etc.).

Right to erasure (right to be forgotten): HR departments need to find the right balance between the obligation to erase data and the need to keep data in case of litigation against employees (need to review applicable rules in connection with statute of limitations).

Right to data portability: Companies will need to organise to deal with upcoming requests in this respect.

Privacy impact assessments: Even though the obligations existed before the GDPR, companies must review their whole process of information and communication to the employees as they need to measure the impact on their privacy right (Privacy Impact Assessment).

Sanctions: Fines of up to 20 million EUR or 4 per cent of company's turnover and possibly, criminal sanctions (5 years of prison / fine of up to 300,000 EUR). In addition to the official sanctions, companies are very sensitive to the possible risks for their reputation as decisions are very often published and commented on social media.

Germany

How is the GDPR being implemented?

As an EU regulation, the GDPR will take direct effect in Germany as of 25 May 2018. Germany has already used the intervening period since 2016 to implement a new Federal Data Protection Act-- the so-called "Data Protection Adaption and Implementation Act" (*Datenschutzanpassungs und Umsetzungsgesetz*), which in May will replace the current Federal Data Protection Act to comply with the GDPR.

What specific rules will be adopted in relation to employee data?

Neither the GDPR nor the new German Federal Data Protection Act adopt specific derogation to the present status of employee data protection in Germany. One of the reasons is that the EU apparently used the old German Data Protection Act as a kind of template for the GDPR. The new Federal Data Protection Act more or less amends the wording to the GDPR. Emphasis can be laid eg, on the word “employee”: In the German act, ”employee” is defined as agency worker, trainee, civil servants and judges, military personnel, alternative service workers and even job applicants (§ 26 Sec. 8 new German Data Protection Act).

Another interesting point is § 26 Sec. 2 new German Data Protection Act: This goes further than Article 7 GDPR and provides that any consent of an employee shall be seen in light of the special relation of a dependent employee of his or her employer. In general, as the old German Data Protection Act has often similar rules, many court decisions exist for problems in connection with company homepages, social media, bring your own devices or the monitoring of employees.

What do HR departments see as the main challenges?

Intra-group data transfers: Especially in multinational companies, data transfer to affiliates or subsidiaries must be observed. Without provisions in the labour and employment contracts or in a works agreement, any transfer is at risk of violating the law. As mentioned, in all member states employee’s consent for any data processing must face fair processing conditions and such processing must be only in connection with employment. Another interesting and yet unresolved question is a central HR database in a multinational corporation and HR decision-makers in only one subsidiary of the group.

Fines: All these questions seem at first glance theoretical, however employers fear the high administrative fines stated in Article 83 GDPR.

Brexit: In connection with the UK and the forthcoming Brexit, Article. 44 GDPR should be noted: Any transfer of personnel data to a third country shall take place only if this country complies with the transfer of personnel data as laid down in Chapter 5 of GDPR.

The Netherlands

How is the GDPR implemented?

The GDPR will have direct effect in the Netherlands as a member of the European Union. The Dutch Data Protection Act will be replaced by the GDPR and the Dutch Implementation Act GDPR (currently in draft, but due to take effect on 26 May). The Dutch Government has sought to provide continuity by constructing the (Draft) Implementation Act GDPR in such a way that it resembles the Dutch Data Protection Act where the GDPR delegates responsibilities to the Member States.

What specific rules will be adopted in relation to employee data?

Even though there are no specific articles in relation to employee data under the (Draft) Implementation Act GDPR, the Dutch legislator has provided additional conditions with regard to sensitive or special categories of personal data, including those of employees.

What are the main challenges?

Data concerning health: In principle, the processing of health data is prohibited. However, under the (Draft) Implementation Act GDPR employers are allowed to process health data if this is necessary for compliance with a legal obligation, a collective bargaining agreement (CBA), pensions and retirement rules that provide for

claims/benefits for employees. It is also allowed to process health data if such processing is necessary for the re-integration of an employee due to sickness or disability.

Please note that it is not allowed to process health data if, for instance, an employee calls in sick. In such an event, the employer may only ask for relevant information in order to judge the employee's abilities/expected availability. It is thus not allowed to ask for the cause or the kind of sickness but employers are allowed to ask employees when they expect to return to work.

Data relating to criminal convictions and offences: Under the (Draft) Implementation Act GDPR it is prohibited to process personal data relating to criminal convictions and offences. Depending on the function of the employee, a pre-employment screening as well as the provision of a certificate of good conduct may be allowed. For instance, this is the case with security, police, teachers or day care employees. It is, however, recommended to assess this on a case by case basis.

Processing personal identification numbers (social security numbers): In principle it is prohibited to process the citizen service numbers unless such processing is explicitly prescribed by law. An example: when an employee is to enter into an employment relationship, it is allowed to make a copy of his or her ID/passport, including the social security number, for identification and for tax purposes.

Processing biometric data of employees: It is prohibited to process biometric data of employees unless the biometric data are processed to uniquely identify the employee and only if this is necessary and proportional for authentication or security purposes. An example of a legitimate interest would be the usage of finger prints or a face scan, for example in order for employees to access construction work sites.

United Kingdom

How is the GDPR being implemented?

While the UK remains a member of the EU this will have "direct effect". Once the UK leaves the EU its operative provisions will be translated into UK law via the combination of a new Data Protection Act, which is currently progressing through Parliament, and an EU Withdrawal Act (currently also a bill) which will translate all directly effective EU law into UK law at the point the UK leaves the EU. That wholesale incorporation will still require some contextual changes, and there will be a schedule spelling out the necessary modifications to the GDPR post Brexit in the new Data Protection Act. These will not alter data subjects' rights, but will make the necessary consequential changes to reflect the UK's new status as a non-member state following its withdrawal from the EU.

What specific rules will be adopted in relation to employee data?

The new Data Protection Act, among other things, will set out the specific conditions for processing special categories of personal data for employment purposes. The conditions will require the employer to have an appropriate policy in place. It will also have to comply with certain additional safeguards which will involve enhanced record keeping obligations.

What do HR departments regard are the main challenges?

Sensitive/special category data: Currently many UK employers rely on consent at least as a fall-back for lawful processing. In the future an increasingly restrictive interpretation of consent is going to mean that employers will need to rely on other fair processing conditions in most circumstances. The new Data Protection Act will provide for a specific exemption for processing which is "necessary for the purposes of performing or exercising obligations or rights" imposed or conferred by law on the data controller "in connection with employment". However, as noted above, enhanced record keeping obligations will now be applied to employers relying on this condition.

Fair processing notices: Not only will these need to reflect the wider range of rights conferred on data subjects under the new regime, but will also have to include a more comprehensive account of how and why the employer processes employee data. Currently the use of fair processing notices is fairly limited in relation to employee data, with employers preferring to rely on generic statements in HR policies or even in contracts of employment.

Subject access requests: Employers will need to ensure that they are able to cope with subject access requests within the new time frame (a month instead of 40 days) as well as having the capacity to respond to any upsurge in the volume of requests due to the abolition of fees. They will also need comply with the new "portability" requirement when providing the data.

Contributors' details

France

Antoine Jouhet
Partner, Labour and Employment
FIDAL
http://www.fidal.com/en/index.php

Germany

Dr. Holger Kühl, LL.M.
Rechtsanwalt
Fachanwalt für Arbeitsrecht
Graf von Westphalen
http://www.gvw.com/en.html

The Netherlands

Emma van Dijk
Advocaat, Arbeid & Pensioen
Van Benthem & Keulen
https://www.vbk.nl/en/

UK

Charles Pigott
Professional support lawyer, employment
Mills & Reeve