BEERG AMEERG
The Brussels European Employee Relations Group
Africa Middle East Employee Relations Group
Perspectives
No. 4, 2015

NEW EU DATA LAW SET TO INCREASE 'RED TAPE' FOR EMPLOYERS

The new EU data protection regulation threatens to increase rather than reduce 'red tape' for employers, primarily because employee data is excluded from the main benefits of 'one-stop-shop' at the heart of the proposed regulation, claim Derek Mooney and Tom Hayes of BEERG, a network of employee relations in transnational companies.

In January 2012 the then EU Commission Vice-President and Justice Commissioner, Ms Viviane Reding, published the draft of a new General Data Protection Regulation (GDPR).

One of her core arguments justifying the new measure was that EU Member States had been implementing the 1995 Directive differently, resulting in divergences in enforcement and uneven data protection laws across the EU. A single law, by way of Regulation, she argued, would create a one-stop-shop, having both uniform effect and implementation across all member states (unlike a Directive which can be adjusted by individual national legislatures when being transposed)

Thus, she asserted, a regulation would do away with fragmentation and costly administrative burdens and lead to savings for businesses of €2.3 billion a year. This €2.3 billion savings figure is key to the rationale for the GDPR and is still being quoted to this day.

In their June 15 joint statement[1] marking the start of talks on the GDPR under the 'trilogue' system (the final stage in the EU legislative process where the EU's Parliament, Council and Commission negotiate a final compromise text), Andrus Ansip, the EU Commission Vice-President for the Digital Single Market, and Věra Jourová, the EU Commissioner for Justice, Consumers and Gender Equality repeated the figure, saying (their emphasis in bold):

> ***One continent, one law*** *– the regulation will establish a* ***single set of rules*** *on data protection, valid across the EU. Companies will deal with one law, not 28. This will save businesses around €2.3 billion a year. In addition, the new rules will* ***particularly benefit small and medium-sized enterprises (SMEs)****, reducing red tape for them. Unnecessary administrative requirements, such as notification requirements for companies, will be removed: this measure alone will save them €130 million per year.*

If only this were the case. The sad truth is that in the employment sphere, the old patchwork of 28 systems will continue, with the added benefit of a raft of additional burdens.

'COP-OUT CLAUSE'

The reason for this is the inclusion of a 'cop-out clause': Article 82 covering the employment context. We in BEERG have been repeatedly and consistently highlighting

[1] http://europa.eu/rapid/press-release_IP-15-5176_en.htm?locale=en

this glaring anomaly since early 1982.bArticle 82 (as it appeared in the original Commission draft) states that:

1. *Within the limits of this Regulation, Member States may adopt by law specific rules regulating the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.*

This means that the entire area of employee data is excluded from the EU-wide "one stop shop". The GDPR specifically provides that each member state shall also be empowered to regulate in this area.

All employers, be they large, medium or small, must process employee data as part of their daily routine. The maintenance and processing of employee data is essential to the effective management of any enterprise. Indeed, for the bulk of companies operating in the EU, their employee database is their biggest database.

Yet, the Art 82 provision means that business will have the patchwork of 28 different rules in 28 countries plus the additional obligations and burdens set out elsewhere in the GDPR (and addressed later in this article) such as Data Protection Officers; consent rules and the potential 2% penalty on annual turnover.

So far from saving business €2.3bn, this measure will cost business at a time when various EU national governments are committing themselves to reducing employment costs.

OVER €3BN IN EXTRA COSTS

We in BEERG have conservatively estimated this additional cost at €3+ billion. This figure is based on the reasonable assumption (based on feedback from our members on the costs incurred in "live projects") that large transnational companies, on average, undertake three employee-data projects per year (over and above day-to-day processing).

Such projects arise from the need to incorporate new acquisitions into existing data systems, upgrading out-of-date software or strengthening systems to withstand hacking or infections.

The inclusion of a provision to allow Member States adopt additional rules over and above those provided for in the Regulation fundamentally undermines the raison d'être of a regulation: which is to have the same rules applying in every EU Member State without variation.

Our concerns at the negative impacts of Article 82 have not abetted over the last three years of legislative scrutiny by the Council of Justice and Home Affairs Ministers and, in particular, by the European Parliament.

Indeed, the direction of travel in the consideration of Article 82 has gone the other way. Instead of looking to include employee data in the one-stop shop mechanism, the Parliament sought to impose greater restrictions and burdens.

Following its deliberations on Article 82, the EU Parliament produced a draft text that considerably expanded on the original Commission draft, adding several extra clauses that amount to 760 additional words (*See full text at end of this piece*).

These provide for, among other things:

- Data processing must be linked to the reason it was collected for, with no profiling or secondary uses;
- Employee consent for the processing of data by the employer is not enough, if the consent has not been given freely;
- No processing of employee data without the employee's knowledge;
- Monitoring of areas such as bathrooms, changing rooms, rest areas, and bedrooms would be prohibited and clandestine surveillance would be inadmissible under all circumstances;
- Special restrictions on the use of personal data in the context of medical examinations and/or aptitude tests and a prohibition on collecting data for genetic testing as a matter of principle;
- Restrictions on personal data arising from the employee's use of the employer's telecommunications facilities for private purposes;
- Personal data on political orientation and/or union activity could not be used to draw up 'blacklists' and the passing on of such lists would be prohibited, with member states conducting checks and adopting sanctions against the use of such lists;

The Council's amended version of Article 82 remains broadly in line with the original Commission draft:

1. *Member States may adopt by law specific rules* ***or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of*** *the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work,* ***equality and diversity in the workplace****, health and safety at work,* ***protection of employer's or customer's property*** *and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.*

We have the gravest concerns as to what compromise the Commission, Council and Parliament representatives will reach in their Trilogue negotiations over the coming six months when faced with the various versions of Article 82.

'PARK' IT FOR FIVE YEARS

BEERG believes that the EU needs to consider how the enactment of any version of Article 82 stands alongside its negotiation of the vital TTIP agreement. We suggest that Article 82 be parked and not come into force until at least three years after the Regulation generally comes into force.

During that five-year period, the European Commission should consult with the social partners in accordance with the Treaty provisions on proposals for a Regulation to cover the processing of data in the employment context.

As we said earlier, Article 82 is not the only provision within the GDPR which should concern those considering the employment aspects of the regulation.

We believe the **Article 7** "consent" requirements for employment related data is over-restrictive. We believe that the consent of employees, or prospective employees, for

such personal data processing, is essential to the employment relationship should be taken as a given.

It should not be necessary to ask for consent every time it is necessary to make changes to company's human resource related personal data processing systems. We do acknowledge, however, that the member states in Council have made some movement on this measure in the context of adopting a "risk based" approach in their consideration of the regulation.

Similarly we feel the **Article 32** provisions on the Communication of Personal Breach requirements in the employment context are excessive. Employers should be allowed to fulfil such communication requirements with respect to employment-related personal data with general notices to all EU employees *en masse,* using whatever means is reasonable.

'DATA PROTECTION OFFICERS'

One area where we are pleased to see the Council has made progress, particularly during the Irish EU Presidency, concerns the Articles 35- 37 provisions on the appointment of Data Protection Officers in enterprises with more than 250 employees.

The Council-amended text now makes this a voluntary requirement and only mandatory where already required by national law. This is a sensible change from the original Commission proposal, but once again we would have concerns as to where a compromise may be reached – given that the original Commission draft and the amended Parliament drafts still seek to make the appointment of DPOs compulsory without any consideration of how much each Data Protection Officer will cost by way of salary, office facilities, administrative staff and an operational budget?

Indeed, due to Article 82 providing for up to 28 different employee-data regimes, a transnational company probably will not be able to get by with just one DPO. How could a DPO in the Netherlands deal with a complaint from a Spanish employee if the laws in Spain are different from the laws in the Netherlands?

Since 2012 the public and political debate on the GDPR has largely centred on how it will impact the major IT and social media companies. The underlying assumption has been that all data and meta-data is the same and should be treated the same – whether it is posting an injudicious photo on social media or holding data on an employee's bank details so that salaries may be paid direct to their bank account.

Regrettably, there has been insufficient discussion on how this measure will affect every employer and company which holds employee data.

In order to employ people, companies need to process essential human resources data, but the range and scope of that data is enormous and includes:

- management and employee communications and notices;
- emergency contacts;
- performance feedback, and progression; succession planning;
- travel and expense reimbursement, including travel and/or credit card administration;
- tax reporting and withholdings;
- planning and provision of health services, including drug screenings;
- visas, licenses and other right-to-work authorizations;

- identification of persons via photographs or other likenesses to ensure visual identification of employees for badges or internal communications;

The management and processing of this essential data is already costly and burdensome, indeed much of the data held is on foot of statutory requirements.

HEALTH AND SAFETY MODEL

Employee data protections should follow the same broad approach as health and safety law. Companies are generally not required to register with health and safety authorities nor do they need prior permission to change systems. However, where they break the rules they are rightly penalised and admonished.

Requiring prior approval, as the GDPR seeks to do, is unnecessary and overly burdensome.

Not only does it inhibit companies in making changes necessary to safeguard their competitive position in the global marketplace, such is the speed of change in today's world that data processing systems are being constantly changed or modified. Supervisory authorities simply do not have the resources to be able to react with the required speed.

Unless the GDPR takes heed of these realities as they relate to its employee data implications, its net impact will be to increase employment costs and further damage European competitiveness.

July 2015

This piece, written by BEERG's Derek Mooney and Tom Hayes, originally appeared in IRN Issue No. 29, July 29th, 2015 www.irn.ie

Compare and contrast GDPR Article 82 sections:

Commission *Original draft*	***Parliament*** *changed/additional parts in bold*	***Council*** *changed/additional parts in bold*
1. Within the limits of this Regulation, Member States may adopt by law specific rules regulating the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.	***1. In accordance with the rules set out in this Regulation, and taking into account the principle of proportionality,*** *adopt by* ***legal provisions*** *specific rules regulating the processing of employees' personal data in the employment context, in particular* ***but not limited*** *to the purposes of the recruitment* ***and job applications within the group of undertakings,*** *the performance of the contract of employment, including discharge of obligations laid down by law* ***and*** *by collective agreements,* ***in accordance with national law and practice, management,*** *planning and organisation of work, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.* ***Member States may allow for collective agreements to further specify the provisions set out in this Article.*** ***1a. The purpose of processing such data must be linked to the reason it was collected for and stay within the context of employment. Profiling or use for secondary purposes shall not be allowed.*** ***1b. Consent of an employee shall not provide a legal basis for the processing of data by the employer when the consent has not been given freely.*** ***1c. Notwithstanding the other provisions of this Regulation, the legal provisions of Member States referred to in paragraph 1 shall include at least the following minimum standards:*** ***(a) the processing of employee data without the employees' knowledge shall not be permitted.***	*1. Member States may adopt by law specific rules* ***or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of*** *the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work,* ***equality and diversity in the workplace****, health and safety at work,* ***protection of employer's or customer's property*** *and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.*

	Notwithstanding the first sentence, Member States may, by law, provide for the admissibility of this practice, by setting appropriate deadlines for the deletion of data, providing there exists a suspicion based on factual indications that must be documented that the employee has committed a crime or serious dereliction of duty in the employment context, providing also the collection of data is necessary to clarify the matter and providing finally the nature and extent of this data collection are necessary and proportionate to the purpose for which it is intended. The privacy and private lives of employees shall be protected at all times. The investigation shall be carried out by the competent authority; ***(b) the open optical-electronic and/or open acoustic-electronic monitoring of parts of an undertaking which are not accessible to the public and are used primarily by employees for private activities, especially in bathrooms, changing rooms, rest areas, and bedrooms, shall be prohibited. Clandestine surveillance shall be inadmissible under all circumstances;*** ***(c) where undertakings or authorities collect and process personal data in the context of medical examinations and/or aptitude tests, they must explain to the applicant or employee beforehand the purpose for which these data are being used, and ensure that afterwards they are provided with these those data together with the results, and that they receive an explanation of their significance on request. Data collection for the purpose of genetic testing and analyses shall be prohibited as a matter of principle;*** ***(d) Whether and to what extent the use of telephone, e-mail, internet and other***	

	telecommunications services shall also be permitted for private use may be regulated by collective agreement. Where there is no regulation by collective agreement, the employer shall reach an agreement on this matter directly with the employee. In so far as private use is permitted, the processing of accumulated traffic data shall be permitted in particular to ensure data security, to ensure the proper operation of telecommunications networks and telecommunications services and for billing purposes. ***Notwithstanding the third sentence, Member States may, by law, provide for the admissibility of this practice, by setting appropriate deadlines for the deletion of data, providing there exists a suspicion based on factual indications that must be documented that the employee has committed a crime or serious dereliction of duty in the employment context, providing also the collection of data is necessary to clarify the matter and providing finally the nature and extent of this data collection are necessary and proportionate to the purpose for which it is intended. The privacy and private lives of employees shall be protected at all times. The investigation shall be carried out by the competent authority;*** ***(e) workers' personal data, especially sensitive data such as political orientation and membership of and activities in trade unions, may under no circumstances be used to put workers on so-called 'blacklists' and to vet or bar them from future employment. The processing, the use in the employment context, the drawing-up and passing-on of blacklists of employees or other forms of discrimination shall be prohibited. Member States shall conduct checks and***	

	adopt adequate sanctions in accordance with Article 79(6) to ensure effective implementation of this point. ***1d. Transmission and processing of personal employee data between legally independent undertakings within a group of undertakings and with professionals providing legal and tax advice shall be permitted, providing it is relevant to the operation of the business and is used for the conduct of specific operations or administrative procedures and is not contrary to the interests and fundamental rights of the person concerned which are worthy of protection. Where employee data are transmitted to a third country and/or to an international organization, Chapter V shall apply***	