Employment Law - General Data Protection Regulation

NATALINO CARUANA DE BRINCAT

In light of the new GDPR Regulations which will come into effect later this month, this article looks at the possible effect that these regulations may have on the Employment sector.

Natalino Caruana de Brincat has successfully completed the Doctor of Laws (LL.D.) degree at the University of Malta. He also holds a Bachelor of Laws (LL.B.) degree together with a Diploma Notary Public awarded by the same University of Malta, whilst is in possession of Master's degree in Business Administration (MBA) from the University of Leicester. He is a founding member of the Junior Chamber of Advocates. He is currently reading for a Doctor of Philosophy (PhD) degree at the University of Malta.

TAGS: Employment Law, European Law, Data Protection Law

Edition: 2017

Citation: Natalino Caruana De Brincat, 'Employment Law - General Data Protection Regulation' (GħSL Online Law Journal, 14 May 2018, <http://lawjournal.ghsl.org/en/articles/articles/82/employment-law---general-data-protection-regulation.htm> accessed **insert date)**

OLJ ONLINE LAW JOURNAL

GħSL Għaqda Studenti tal-Liġi

1. Introduction

This article will shed light on the broad applicability of the General Data Protection Regulation (the "GDPR" or "Regulation") in employment.

On the 25 May 2018, the GDPR will transform how business operations are executed in Malta, as in the rest of the EU. The GDPR`s main focus is to shield individuals from the abuse of data handed over to third parties, having as its aim stored information which can be used to identify an individual.[1]

The Regulation will automatically become effective as from the above-mentioned date. The GDPR will also be enforced in Malta by the Information and Data Protection Commissioner,[2] (under the Regulation referred to as the supervisory authority) (referred hereinafter as the "Commissioner") who is empowered to implement the Regulation across the Maltese Islands. The Regulation will replace the Data Protection Directive (1995)[3] (the "Directive") which was introduced at a time when the internet was still not so widely available. Thus, data collection and storage was not its primary focal point.

1 Regulation (EU) 2016/679 of The European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

2 Data Protection Act Chapter 440 of the Laws of Malta – Article 2 - "Commissioner" means the Information and Data Protection Commissioner appointed under article 36 and includes any officer or employee of the Commissioner authorised by him in that behalf;'

3 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

The Commissioner is also charged to act as the one stop office and to clarify matters related to the GDPR, whilst being given quasi-judicial functions by being assigned the powers to issue administrative fines.[4]

The salient changes to rules concerning data protection will shift the current goal posts, especially in issues relating to administrative fines, which can now go up to four per cent (4%) of global turnover or twenty million (€20,000,000), whichever is higher, for operations which are found in breach of the GDPR and hence found incompliant therewith. The changes to data protection brought about by this Regulation are intended to strengthen the rights of the Data Subject,[5] which are a fundamental pillar of the Europe Union (EU), and which provide individuals with the appropriate comfort to trust third parties who are granted access to and processing rights over their personal data.

The GDPR brings about notable changes, in particular to the validity of consent as a legal basis for processing data, the ease of access to one's personal data and the portability thereof, and of utmost importance, the Regulation establishes one`s right to be forgotten is.

2. Mere consent is no longer enough.

It is common practice for employers to rely on a general umbrella consent given by the employee for them to collect and otherwise process information in relation thereto,

4 Regulation (EU) 2016/679 - Article 83 – 'Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive'.

5 Data Subject in this article means a person to whom the personal data relates.

when signing an employment agreement. In matters related to data protection such an open-ended consent clause within an employment agreement was considered to legitimise the processing of employee`s personal data.

The GDPR changes the goal posts, rendering the validity of such an umbrella consent clause more than questionable. Under the Regulation, consent must necessarily be freely granted, informed, specific and unambiguous, for it to be considered a legitimate basis for the processing of personal data, such as that of an employee.[6]

As briefly listed above, the Regulation elaborates on a set of conditions for consent not to be vitiated, thus, being considered as valid consent. Such conditions are far more stringent and onerous than those adoperated under the Directive.[7] Amongst others, these conditions include that an opt-in consent clause must be drafted and presented to individuals in clear, simple and plain language. This implies that such clauses must be to the point, free of technical jargon, ideally in short sentences and without cross-referencing.

Furthermore, the presentation of such consent clauses must be in a manner which is clearly distinguishable from other clauses in an employment agreement (or in any other document as the case may be). It is highly advisable for the data processor seeking such consent to segregate

6 Regulation (EU) 2016/679 – Recital 32 – 'Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. [omissis]'

7 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

clauses dealing with data protection and to present them separately, with a clear title which explicitly distinguishes this from other issues.

The Regulation gives paramount importance to the right to withdraw consent.[8] Therefore, within consent clauses, such as those (as the case may be) in employment agreements, it must also be explained to the Data Subject that they have the right to withdraw such consent.

When the employer is analysing whether consent was freely granted or given by the employee, they should consider whether the data was necessary for the performance of the agreement. If it is necessary, then it is safe to opine that consent is hardly required since the employer can rely on the necessity to fulfil their contractual obligations as a legal basis to process an employee's data, in its own right.

If, however, the data is not so necessary, and consent is nonetheless required from the employee as, let's say, a pre-condition to the employment, then, consent would be vitiated in that the employee had no real choice but to give it if s/he want the job, although the data is not strictly necessary for the employment relationship or in terms of some other legal basis.

Once again, the employer should consider including within the drafting of a consent clause the reasons why consent is so required. It is important for employers not to be over reactive, however an alarm bell should have gone off some time ago to update all documentation and take

8 Regulation (EU) 2016/679 - Article 7 (3) – 'The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.'

stock of the situation.

While employers will still be able to rely on the employees` consent for the processing of personal data, such consent should be separate and distinct from the employment agreement. The consent clause shall be compliant with the Regulation for it to be considered as valid. There shall always be the option available for the employee to grant genuine consent to employer to process their personal data.

Furthermore, processing of 'special categories of personal data',[9] which data includes, amongst others, racial or ethnic origin, political opinions, religious, or trade union membership, must be by 'explicit consent'[10] , implying that when the data falls within such categories the consent clause must be detailed and clearly outline the reasons for processing such data.

It would be advisable for employers to assess the current modes and forms used to gather data from their respective employees and where so required bring these in line with the GDPR requirements to avoid being subjected to the hefty administrative penalties aforementioned.

It is imperative for employers to realise that generic, umbrella consent clauses for all data processing are no longer a viable option since these certainly do not attract effective consent. It would be prudent for employers to seek

9 Regulation (EU) 2016/679 - Article 9 (1) – 'Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.'

10 ibid (n8) Article 9 (2)– 'Paragraph 1 shall not apply if one of the following applies: (s) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes [omissis]'

specific consent from their employees depending on the data being processed and insofar as the data is not being processed in terms of another legal basis.

3. Is legitimate interest a valid cause to process data?

The employer is not hindered from processing data where there exists a legitimate interest.[11] This means that if there is some lawful reason why the data pertaining to the employee is being processed, the employer is not required to obtain the employee's consent.

Nevertheless, the employer is bound to explain what the legitimate interest is, why it is being pursued and the reasons why it gives them the right to process the personal data of the employee. The employer must understand that legitimate interest is not a wild card which trumps over the employee`s rights.

It can be argued that certain personal data processing, such as the recording of an individual's image using CCTV systems, is a necessity. However, in such circumstances the employer is bound to assess his interest, evaluate the level of necessity to securing the work environment, and consider if such outweigh the employees right to privacy.

Necessity can also be considered from the perspective of the fulfilment of the employment agreement obligations and which thus gives rise to an alternative legal basis

11 ibid (n8) Article 6 (1) – 'Processing shall be lawful only if and to the extent that at least one of the following applies: (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child'.

to consent in terms of which an employee`s personal data can be processed.

4. Process data as transparently as possible.

The Regulation stresses greatly on the issue of transparency and clearly links this issue also to employment matters.[12]

In simple words, employers are bound to ensure that employees can be furnished with; (i) details as to the legal basis in terms of which their personal data is being processed[13], (ii) by who and how the data will be processed, who will have access to the data, whether it will be shared with any third parties (these must be explicitly named), confirming that these are GDPR compliant, and also the period the data will be stored for, (iii) all rights available to the data subject[14] including the right to withdraw consent together with the right to be forgotten, and finally (iv) a guide as to how to make a complaint with the Commissioner if so required.

As explained above, the information given to the employee must not be technical in nature, and clear and plain language must be used. It is suggested to avoid long paragraphs which can hinder the employee from understanding his rights. Therefore, the information shall be freely accessible, transparent and concise enough for every em-

12 ibid (n8) Article 88 (2) – 'Those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place.

13 With exceptions depending on the legal basis (you might want to go into this)

14 Data Protection Act Chapter 440 of the Laws of Malta – Article 2 - "data subject" means a natural person to whom the personal data relates;

ployee to understand without requiring assistance from professionals, such as legal counsel.

This implies that employers should seriously consider introducing a data protection policy as part of a comprehensive employees' handbook which provides the aforementioned information. It is advisable that such a handbook or human resources management (HRM) policies are distributed to all employees as part of their induction course. During the induction course the HR Manager or his/her designate should stress on the right to be given information, the right to withdraw consent and finally the right to complain to the Commissioner.

5. Do employers need to engage a data protection officer?

In certain cases, employers are bound to designate someone within their organisation as a data protection officer.[15] It is necessary, therefore, to elect a data protection

15 Regulation (EU) 2016/679 - Article 37 (1) – 'The controller and the processor shall designate a data protection officer in any case where: (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10. (2) A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment. (3) Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size. (4) In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors. (5) The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and prac-

officer if, for example, the core activity of the controller[16] is such that it involves:

> processing operations that require regular and systematic monitoring of the data subjects on a large scale, or where the core activities of the controller or the processor consist of processing on a large scale of special categories of personal data [omissis]. The necessary level of expert knowledge should be determined in particular according to the data processing operations carried out and the protection required for the personal data processed by the controller or the processor. Such data protection officers, whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner.[17]

Hence, an employer who`s main function is processing operations of personal data, such as providing storage facilities on data servers, must employ a designated data protection officer. Nonetheless, in cases of smaller operations it should be sufficient to merely train someone within the firm to deal with issues relating to data protection rather than assigning a data protection officer. In both scenarios the individual so appointed should be qualified and have sound knowledge of data protection legislation. The employer should always assess his operation and take stock of all matters directly or indirectly regulated by the GDPR

tices and the ability to fulfil the tasks referred to in Article 39. (6) The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract. (7) The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

16 Controller in this article means a person who alone or jointly with others determines the purposes and means of the processing of personal data.

17 Regulation (EU) 2016/679 - Recital 97.

before considering his options.

6. Do employers need to notify a breach?

The Regulation provides that an employer must notify the Commissioner of a data breach within a maximum period of seventy two (72) hours from when they become aware of a breach - whether internal or external (such as a cyber-attack, losing a memory stick, phones or laptops with personal data thereon).[18] The notification is not mandatory when the employer is of the opinion that the breach is unlikely to pose a risk to the employees' personal data.[19]

Conversely, if the breach so requires that notification is made to the Commissioner, the employer is bound to explain the nature of personal data breach. In these cases, the employer must give a detailed account of what transpired, list the potential employees affected and explain what the possible repercussions are, the actions being undertaken or a proposal of the measures being considered to address the particular breach.

In the event where the data breach is likely to, directly or indirectly, affect employees, the employer is bound to notify them too without delay. It would be advisable for

18 Regulation (EU) 2016/679 - Article 33 (1) – 'In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.'

19 Regulation (EU) 2016/679 - Recital 85 - '[omissis] unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.'

the employer to explain, in detail, the nature of the breach, the remedies taken, and the rights of the employees at law which include the lodgement of a complaint with the Commissioner.

Employers should consider implementing the appropriate policies to prevent such scenarios. Furthermore, every firm should have a breach notification action plan to be followed in the eventuality a breach is identified. Documentation trail and record keeping is of utmost importance here. The facts and the effects to the personal data due to the breach are to be documented and kept on record permanently. It is also of paramount importance to keep trail of the measures and actions taken to remedy the effects of the breach and avoid further breaches from occurring.

7. What are the penalties attached to violations?

An employer who fails to comply with the Regulation may be subject to substantial administrative penalties. The penalties vary according to the nature, gravity and duration of the infringement taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them.[20] By way of example, infringement related to data subjects' rights can be subject to administrative fines of up to twenty million Euro (€20,000,000), or in the case of an undertaking, up to 4% of the total worldwide annual turnover in the preceding financial year, whichever is higher!

Nevertheless, each Member State should lay down the

20 Regulation (EU) 2016/679 - Article 83 (2)(a).

rules for other penalties applicable to infringements of the Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and take all measures necessary to ensure that they are implemented. Such penalties should be effective, proportionate and dissuasive.

This does not mean that the Commissioner will be acting in isolation, but that, on the contrary, local authorities may be subject to external pressure from their counterparts in other Member States to coordinate their forces and impose higher pecuniary sanctions.

8. Conclusion

In conclusion, the GDPR, changes the way an employer operates from a data protection perspective. The need for such change has been discussed and most employers fear the 25 May 2018, some comparing it to a Trojan horse.

There are a few steps which are crucial for any employer to make sure they are compliant with the Regulation. Firstly, the employer must attend to his internal policies and privacy procedures, ensuring they are in simple and clear language. Secondly, they must make sure that the policies and operational practices are in line with the requirements posed by the Regulation when processing employee's personal data.

Thirdly, they must ensure that their employees are duly notified of their rights at law including the right to withdraw consent and the right to be forgotten. Finally, the employer should issue guidelines and procedures for any eventual data breach, which would include the mode and

time frames of reporting breaches to management and the Commissioner alike. These are but a few tips which one should consider and not an exhaustive list which can be utilised in relation to the GDPR as an employer's tool-box.

Employers' first port of call should be the HR manager so that they can audit the current employee data processing policy. It is imperative for employers to consider GDPR implications seriously, especially when considering that this Regulation has not yet been tested, thus no one has yet opened Pandora's Box.[21]

21 This article cannot be taken or considered as a full illustration of the Maltese Employment Law and of the Regulation (EU) 2016/679 of The European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Employment and Data protection are two of the areas which are vastly regulated by several European Union directives and regulations. (This article was written on the 1st May 2018)