EEF response to call for views on the General Data Protection Regulation derogations.

Overview

1. EEF, the manufacturers' organisation is the voice of manufacturing in the UK, representing all aspects of the manufacturing sector including engineering, aviation, defence, oil and gas, food and chemicals. With some 20,000 members employing almost one million workers, EEF members operate in the UK, Europe and throughout the world.

2. While the call for views refers to derogations we identify a number that would not be considered "exceptions" or "exemptions". Instead of allowing members states the ability to reduce employer/data controller obligations some of the derogations give power to member states to increase the rights of individuals and increase employer/data controller obligations.

3. There are other derogations within this call for views that are rights or obligations that are dependent on member state national law. For example, you can process data about criminal convictions where the processing is authorised by member state law if there are sufficient safeguards. In these cases, the UK Government should consider whether there are circumstances where existing national law needs to be altered, to clarify or extend the freedom of employers to process employment related data in a useful, efficient and fair way and to remove any unwanted consequences arising from the international of such existing national law with the General Data Protection Regulations (GDPR).

4. Below we have provided comment only in the areas of most interest to manufacturers. Overall, we would add that where a loosening of the regulatory burden is not possible, we would recommend maintaining consistency with the DPA provisions insofar as possible, as employers are familiar with these principles. Any changes to the existing regime will entail some increase in costs as employers would need to amend their current systems and processes in order to comply with the new provisions.

5. Unless there is an opportunity to reduce the regulatory burden, we recommend that the Government maintain an approach that is as close as possible to the current law under the DPA – which employers are now familiar with.

Theme 1: Supervisory Authority and Theme 2: Sanctions

6. We would not want the UK to give additional powers to Supervisory Authorities in relation to investigations and sanctions (Article 58) or to provide for any additional penalties (Article 83/84). The sanctions in the GDPR are already very stringent (we would say they are disproportionate) and much harsher than under our current regime.

Theme 3: Demonstrating Compliance

7. In principle, we anticipate that it would be helpful for the Government to establish Codes of Conduct and Certification Bodies if they are voluntary for employers and make compliance simpler and easier to demonstrate. However, the devil will be in the detail and our support of any proposals will depend on their nature and content.

Theme 4: Data Protection Officers

8. We do not want the UK to require the appointment of data protection officers in additional circumstances (a power available to member states under Art 37). While the majority of EEF member companies will not be required to have a data protection officer, they may choose to have someone in that role – it is less burdensome if this is voluntary as the company then has the freedom to designate the tasks and responsibilities it wants to any data protection officer it chooses to appoint.

Theme 7: Sensitive personal data and exceptions

9. Article 9(2)(b) allows the processing of sensitive data that is "necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment…in so far as it is authorised by Union or Member State law" provided there are appropriate safeguards.

10. In accordance with ICO guidance, employers have relied on the equivalent provision under the DPA to process some health related information about employees, for example, to manage employees who are off sick or who require reasonable adjustments because they have an underlying condition. It would be very helpful for employers ultimately to have more certainty that this approach is legally safe. We therefore suggest a review of UK law, to consider if it could be amended to give employers the certainty they need.

11. Article 9(2)(h) allows processing of sensitive data that is "necessary for the purposes of ...occupational medicine, for the assessment of the working capacity of the employee… on the basis of Union or Member State law". Article 9(3) clarifies that the data must be processed under the responsibility of a professional who is subject to the obligation of secrecy under union or Member State law or by another person subject to such laws. Consideration should be given to whether any changes are needed to relevant UK laws to allow employers, occupational health professionals and others to make use of this exception in such a way as to make it easier for employers to use health data to make fair, evidence-based decisions about the management of employees with possible and actual health conditions, and to implement measures to assist them. (Note that the requirement that data be processed "by or under the responsibility of a professional subject to the obligation of professional secrecy" would seem to limit employers' ability to rely on

this condition for processing – most employers wouldn't themselves be under such a secrecy obligation, and occupational health providers (whose medical staff would be under such an obligation) may be reluctant to take on legal responsibility for processing that is being carried out by the employer).

12. Whether or not any changes are made to UK law as a result of such a review, we would welcome specific guidance for employers from the ICO on the circumstances in which they can rely on Articles 9(2)(b) and (h) to process sensitive personal data of employees.

Theme 8: Criminal Convictions

13. Article 10 allows the processing of sensitive data about criminal convictions where the processing is authorised by Member State law, provided there are sufficient safeguards. We would ask Government to review whether our current system (that in certain circumstances allows employers to process information about criminal records of job applicants/employees) has sufficient safeguards in place to comply with this article.

Theme 12: Processing of Data

14. Article 6(c): Processing of non-sensitive data is allowed where this is necessary for compliance with a legal obligation. Article 6(2) allows member states to be more specific about what constitutes a "legal obligation". On balance, in our view it is better to leave the wording as is, i.e. "legal obligation" – since it potentially allows for quite a broad interpretation. This may be more helpful than a prescriptive list and give employers more freedom as to how they use data.

15. Article 35: we would not want to make impact assessments obligatory in more circumstances.

16. Article 88: allows for derogations in the context of employment – but only where they ensure the protection of the data subject's rights and freedoms in respect of processing employees' personal data. Whilst we would welcome any derogations that gave employers more freedom and choice in how they use employee data/records, our understanding is that this derogation can only be used to increase employee rights and protections. Accordingly, making use of the Art 88 derogation would actually decrease employer freedoms in relation to data and increase burdens on employers, so we would recommend against doing so.

Theme 13: Restrictions

17. This theme covers exemptions, allowing Member States to restrict the application of some of the individual rights under the GDPR. The purposes for which exemptions are permitted under Art 23 are essentially the same as those that currently apply under the DPA (e.g. prevention or detection of crime, protection of national security, etc). Accordingly, save where the Government considers that Art 23 might allow for broader exemptions (i.e. greater restriction of individual rights, more freedom for data controllers/ processors), we would recommend maintaining the existing exemptions that apply under the DPA where possible, as employers are used to working within these parameters.

18. Note also that Art 23 is more prescriptive as to how any exemptions must be defined (e.g. requiring the national law introducing the exemption to specify what categories of personal data are covered, safeguards to prevent abuse, storage periods, etc.) and we would therefore welcome guidance from the ICO on the operation of such exemptions, with particular examples relevant to employee data where appropriate.

FOR FURTHER INFORMATION CONTACT:

Follow us online: