Department for Culture Media & Sport, Call for views on the General Data Protection Regulation derogations
CBI submission, May 2017

The CBI welcomes the opportunity to respond to the Department for Culture Media & Sport consultation on the General Data Protection Regulation derogations. We are the UK's leading business organisation, speaking for some 190,000 businesses that together employ around a third of the private sector workforce. Our membership is made up of businesses from all sizes, sectors and regions.

As set out in the CBI's 'The Future of UK Data Protection' paper - data use by business is critical to the UK's economy, innovation landscape and our ability to trade. The UK played an instrumental role in shaping the General Data Protection Regulation (GDPR) and the CBI supports this regulation forming the significant basis of our future data protection regime.

While this consultation addresses specific measures over which the government can exercise flexibility within the GDPR, there are key principles the CBI advocates the government should consider when shaping the implementation of the regulation:

- **The GDPR presents a harmonised framework for data protection across the EU. Where possible, derogations should be co-ordinated so that there is limited divergence across member states which will benefit cross border trade and reduce red tape.**
- **The derogations that the UK government should exercise power over should focus on ensuring that businesses can remain competitive, continue delivering innovative products and services and carry out contracts.**
- **The government should work towards ensuring that the UK's data protection regime is favourable to achieving a future UK-EU data deal.**

The CBI submission focuses on the themes and related derogations which businesses have highlighted as a priority.

Theme 1: Supervisory Authority

The ICO must be an independent, well-resourced and objective regulator.

Article 52:

The ICO will need significant resources and infrastructure in order to effectively regulate the GDPR. Businesses welcome that in recent months the ICO has increased its staffing capacity and has stepped-up implementation activity. Businesses would appreciate clarity from the government on the funding structure for the ICO and support the current direction of travel towards a tiered data protection fee. Government should make sure that enforcement activity is not a revenue stream for the ICO as relying on that mechanism will create unbalanced incentives for regulator activity.

Theme 4: Data Protection Officers

Government should not specify a requirement for all businesses to appoint a data protection officer.

Article 37:

The UK government should not designate the need for 5.4 million UK businesses to have a data protection officer. While this will be an important job role for many firms, it is not necessary and overly burdensome for all UK businesses to have a data protection officer.

Recommended actions for government:

- Government should not introduce a requirement for additional data protection officers to be appointed in cases other than those referred to in Article 37

Businesses require additional clarity around the triggers for controllers and processors designating a data protection officer. This is important for firms given the potential exposure to a Tier 2 breach fine for a failure to appoint a data protection officer where required. In particular, more guidance around what constitutes “core activities of regular/systematic monitoring of data subjects on a large scale” and “core activities of processing on a large scale of special categories of data”.

Theme 4: Archiving and research

Enabling the processing of data in relation to scientific, historical and statistical purposes is key to supporting the UK’s innovation landscape.

Article 89:

Business access to and processing of data in relation to scientific, historical and statistical purposes is a crucial activity which is essential for many different types of innovation. For example, processing these special categories of data are vital for R&D activities which provide growth for the UK economy and is a key strand of the UK’s Industrial Strategy.

The UK government should ensure that the existing legal protections for processing these special categories of data are retained under the GDPR.

Recommended actions for government:

- The government should retain Section 33 (Research and Statistics) of the 1998 Data Protection Act
- The government should retain Statutory Instrument 2000 No. 417

Theme 7: Sensitive personal data and exemptions

Processing sensitive personal data is fundamental to the services and products that businesses deliver for consumers. Government must ensure that there is a clear legal basis to process this type of data.

Article 9:

The processing of sensitive personal data, ranging from health, to biometric and types of employment data, is crucial to a wide array of industries and business obligations. Processing this type of data is fundamental to a range of products and services that businesses deliver. For example, the ability for insurance firms to offer health insurance, retailers to provide tailored services based on lifestyle information or businesses to conduct due-diligence checks.

Under the GDPR and following draft ICO guidance, the use of explicit consent appears not to be reliable grounds for processing sensitive data. The draft ICO guidance states: “if you require someone to agree to processing as a condition of service, consent is unlikely to be the most appropriate lawful basis for the processing."

This interpretation has significant implications for the ability of businesses to continue offering core products and services that have previously relied on explicit consent as the basis for processing sensitive data. For example, contracts within the insurance industry (e.g health, travel and life) are based upon consent of their customers. Where consent is not the appropriate legal basis to process this data, government must take action to provide new legal conditions.

The CBI supports the government legislating to provide additional legal bases to process sensitive personal data. This is crucial for when processing the data is necessary to fulfil a contract or when the processing of sensitive data is the entire basis of the product or service that the data subject has chosen to engage with.

Recommended actions for government:

- The government should ensure that existing legal justifications from the 1998 Data Protection Act are carried forward under the GDPR.
- The government should ensure that provisions within the Statutory Instrument 2000 No. 417 (and any other appropriate sensitive data orders) that permit the processing of special categories of data are carried forward under the GDPR. This is important for enabling the processing of data by one individual on behalf of another.
- The Government should legislate to provide businesses a legal basis to process special categories of personal data, particularly where such data is also necessary to perform a contract.
- The government should not introduce further restrictions under Article 9 to processing sensitive data.

The government should also ensure that the processing of sensitive data is legitimate in an employment context. For example, but not limited to, employee vetting, biometric processing and diversity monitoring. The government should ensure that the processing of sensitive data is legitimate in a due-diligence context, for example, but not limited to, crime prevention (investigation and prosecution), anti-money laundering, and counter-terrorism.

Theme 8: Criminal convictions

Processing security and criminal convictions data is essential for businesses. Government must ensure that there is a clear legal basis to process this type of data.

Article 10:

The processing of personal data related to criminal convictions or related security measures is crucial to many industries such as financial services, insurance, credit and professional services. Similar to Article 9, the use of this data is essential in both employment contexts (employee vetting, employee security monitoring) and due-diligence (anti-money laundering, crime prevention, KYC checks, fraud prevention).

As this type of personal data has been made a distinct category within the GDPR, it is essential that the government ensures that there are laws with safeguards in place so that legitimate uses of this type of data are able to continue. Both by businesses who directly process the data, such as financial services firms, but also third parties and professional services firms who carry out due-diligence checks on behalf of clients.

The CBI supports the government legislating to provide a legal basis for businesses to process criminal and security data.

Recommended actions for government:

- The government should take into consideration the gaps that exist in UK law due to criminal convictions data now being a separate category and the implications this has for the legal grounds to process this data.
- Where possible, the government should ensure that existing legal justifications from the 1998 Data Protection Act are carried forward under the GDPR.
- The government should ensure that there are legal conditions for businesses to process personal data related to criminal convictions or related security measures in an employment context, for due-diligence, perform a contract and when it is a legitimate interest of the business to process such data to prevent and detect fraud.

Theme 9: Rights and Remedies

Data subjects' rights must be balanced against other business and legal obligations.

Article 17:

The CBI believes that existing UK laws, alongside ECJ rulings, have established a strong 'Right to be forgotten' principle which is balanced against other rights. Existing UK laws should cover the necessary exemptions and so the CBI supports the UK government not introducing additional legal obligations through the form of derogations.

Recommended actions for government:

- The government should not introduce new legal exemptions for the 'Right to be forgotten'

Article 22:

The CBI believes that there should be exemptions to the right for individuals not to be subject to a decision based solely on automated processing, including profiling and supports the government legislating to provide these exemptions and their associated safeguards. This type of processing is essential to a range of core products and services that businesses offer and is particularly important for carrying out due-diligence obligations.

Recommended actions for government:

- The government should ensure that where automated decisions are made as part of risk assessment, corporate due diligence (e.g. checking data subjects against watch lists) and the performance of a contract (e.g. travel insurance) that these practices continue to have a legal basis.
- The government should ensure that where the processing of sensitive personal data is necessary for a contract or automated decision (e.g quoting for an insurance product), that this automated processing has a legal basis.

It is important to recognise that businesses have numerous safeguards in place for decisions made on the basis of automated processing, namely that there is often an element of human intervention. For example, in the due-diligence context where a data subject is flagged against a watch list, it is likely that an individual would check this process before a final decision is made. Government should ensure that automated decisions that have an element of human intervention have a clear legal basis.

The government should also take action so that there are legal safeguards to protect innovative uses of profiling. Profiling and general aggregation of customer data is crucial to many industries and the development of new products and services. For example, in the energy sector the ability to use smart metering technology to assist with energy efficiency measures and reducing tariffs is based upon profiling.

Businesses would also welcome additional clarity from the UK government on the basis for which profiling is permitted in relation to children's data. For example, whether there is a need for more legal certainty to authorise an automated decision based on the processing of children's data (e.g. a family travel insurance quote).

Theme 10: Processing of children's personal data by online services

Businesses support the age of consent for children's access to online services remaining at 13.

Article 8**:**

The CBI supports the UK government keeping the age of consent for children's access to online services at the age of 13. Access to online services provides important social and economic benefits for children, particularly in the development of digital skills, literacy and resilience. A higher age of consent presumes that online activities are inherently risky and creates tension with the overall aim of creating a safe digital ecosystem for all. The CBI supports the work of educational groups, child safety experts and anti-bullying

organisations that have published evidence indicating that the age of data protection consent should be set at 13.

Recommended actions for government:

- The government should keep the age of consent for children's access to online services at 13

Businesses encourage the UK government to push for harmonisation across the EU for the age of consent to be set at 13. This is important for ensuring commonalities in practices and standards across the EU and encourages the development of digital literacy. However, while the principle of harmonisation is important, it should not come at the expense of the UK setting the age of consent at 13.

Theme 13: Restrictions

Government should ensure that the current exemptions from the 1998 Data Protection Act are retained for the GDPR.

Article 23:

The CBI supports government legislating in specific situations to restrict the applicability of data subject's rights. For example, access to non-public credit reference agency data is crucial to ensuring the fair and effective recovery of public sector debt. Existing exemptions within the 1998 Data Protection Act ensure that the rights of data subjects do not go unfettered but are necessarily and proportionately balanced against the public interest of a properly functioning tax and judicial system.

Government should also take steps so that there are legal parameters that protect the disclosure of intellectual property and trade secrets under GDPR which is crucial to business competitiveness. For example, the logic and data used for conducting automated individual decision making will often be bespoke to the business and thus the intellectual property of the firm. Businesses would welcome government providing safeguards so that companies are not forced to disclose information which would damage their intellectual property and ability to compete.

Recommended actions for government:

- As a minimum, the current exemptions in the 1998 Data Protection Act should be retained for the GDPR.