Department
for Culture
Media & Sport

Derogations consultation

2 messages

Dear Sir/Madam

We are unable to submit this using your online tool as it does not appear to be working and we note the consultation closes today. Please therefore accept our response by email. We would be grateful if you could acknowledge your acceptance of our participation in the consultation.

We wish to respond and theme 8 and secondly make general comments about derogations:

Theme 8

Dun & Bradstreet is the world's leading source of business information and insight. Since 1841, Dun & Bradstreet has collected information about businesses to deliver products and services that assist our customers in making critical commercial decisions. Dun & Bradstreet's global business database contains more than 265 million business records, which we compile through a wide variety of partners and public sources. Some of the information we collect may be classed as “personal data” under EU law as it is information relating to an individual (e.g a sole trader, a partnership, a company director, a beneficial owner, a trustee, a professional contact etc). Because we process Personal Data we have been operating a significant programme to ensure compliance with the GDPR. One significant area for which clarification is needed concerns the processing of criminal convictions.

As background, D&B processes data so that it can supply commercial data about businesses and organizations to other businesses on their credit history, business-to-business sales and marketing, counterparty risk exposure and supply chain management. The purpose of this processing is to enable businesses to manage their financial risks, know who they are doing business with, meet compliance obligations and better understand industries and markets. The business information that we collect includes the following:

- Company and business professional contact information, including name, title, address, phone number, fax number, and e-mail address, domain names, and trade associations;
- Detailed company profiles and statistics, including number of employees;
- Background information regarding company management, such as beneficial ownership/persons of significant control, the educational and career histories of company principals;
- Company operational histories, including territories, subsidiaries, affiliates, and lines of business;
- Detailed trade and business credit information, including payment histories and patterns;
- Summary business information regarding profitability, debts, assets, net worth, and business relationships;

- Business compliance information from public source government and professional records, media and business publications
- IP addresses

However our compliance-related products (including Compliance Check™ and Onboard™) may also include information relating to criminal convictions. We assist our customers in complying with various Anti Money Laundering and Know your Customer obligations. A key part of this is whether their target has criminal convictions for relevant matters (fraud, terrorism etc)

As you are no doubt aware, under current law, crime-related data is included in the definition of "sensitive personal data", and explicit consent is available as a lawful ground for processing. However, in the GDPR, crime-related data is not included in the "special categories of personal data," and is instead dealt with in Article 10. Therefore under the GDPR, explicit consent is not available as a lawful ground for processing crime-related data**,** and any such processing will need to comply with Article 10.

Therefore it is critical for us as a business to have a clearer overview of what is meant by:

- Under the control of official authority; and
- When the processing is authorised by EU or Member State law providing for appropriate safeguards for the right and freedoms of data subjects

For processing to be 'authorised' suggests UK law must explicitly provide that such crime-related data can be processed. We are aware that one law that authorises such data processing is anti-money laundering ("**AML**") regulation. In the EU, the relevant law on AML is the Third Anti-Money Laundering Directive (2005/60/EC) ("**MLD3**") which will be amended and replaced by the Fourth Anti-Money Laundering Directive (2015/849) ("**MLD4**") from 26 June 2017. Interpreting the GDPR with MLD4 it is possible to argue that

- Our customers (that are obliged entities under MLD4) must be able to process crime-related data (convictions and allegations of criminal activity) to comply with their obligations under MLD4; and
- We should not be prevented from processing crime-related data in order to efficiently assist such obliged entities since this reflects the general public interest.

However, there is scope for uncertainty here, and as a responsible business we feel we would wish to seek the support and engage with the “official authority” to oversee the processing of our crime-related data.

Under the control of official authority

We feel it is significant that the phrase 'under the *control* of official authority' appears in Article 10 of the GDPR but in no other provision of the GDPR. Elsewhere in the GDPR there are references to 'in the *exercise* of official authority' where the official authority is usually vested in the controller. There was clearly a deliberate decision to use 'under the control of official authority' in order to mean something different from 'in the exercise of official authority'.

“Control” implies a degree of direction from an official authority. The reference to official authority indicates a degree of Government involvement or Government sanctioned authority (e.g. regulatory body or law enforcement agency). We further feel it is significant that the final sentence in Article 10 states that '*any comprehensive register of criminal convictions shall be kept only under the control of official authority*'.

Consequently carrying out processing under the 'control' of official authority in the first sentence in Article 10 suggests that the data is not necessarily 'kept' or stored by the official authority since the drafters would otherwise have expressly required that. Control must mean, as a minimum, that the controller has notified the official authority that it wishes to process crime-related data and that official authority has the power to decide (or at the very least oversee) such processing activities

We have heard anecdotally that the “official authority” for the UK will be the Home Office and not the ICO. Bearing in mind implementation of the GDPR is 12 months away we can only urge the Government to put in place procedures to manage the “official authority” so the legitimate business interest of companies such as ours is not interrupted.

All themes - Derogations Generally

One of the aims of the GDPR is to have one single pan-European set of rules instead of the 28 national laws today. The GDPR also seeks to create a level playing field between EU and foreign companies in that foreign companies based outside the EU will have to apply the same rules as European companies.

We feel however that Member State derogations contradict these aims and could be an unjustified restriction on the free movement of data, which will constrain the development of the EU data economy.

A Communication from the Commission to the European Parliament etc entitled “Building a European Data Economy” states (pg 7):

“The principle of free movement of personal data enshrined in primary and secondary law should also apply in the cases where the GDPR allows Member States to regulate specific matters. Member States should be encouraged not to make use of the opening clauses in the GDPR to further restrict the free flow of data”

As an international company with a significant UK presence we welcome the opportunity the GDPR brings to make doing business across the EU consistent and urge the UK Government not to introduce derogations that contradict this unnecessarily.

dun & bradstreet

Dun & Bradstreet Limited is authorised and regulated by the Financial Conduct Authority.

11 May 2017 at 14:50