RELX Group

RELX Group submission to the Government's 'Call for Views' on GDPR implementation

10 May 2017

Who we are

RELX Group is a FTSE 30 UK-based provider of information and analytics for professional and business customers across industries.

We help scientists make new discoveries, lawyers win cases, doctors save lives and insurance companies offer customers lower prices. We save taxpayers and consumers money by preventing fraud and help executives forge commercial relationships with their clients. In short, we enable our customers to make better decisions, get better results and be more productive. We do this by leveraging a deep understanding of our customers to create services which combine information and data with analytics and technology in global platforms.

We serve customers in more than 180 countries and have offices in about 90 countries. Our headquarters is in the UK where we employ nearly 5,000 people in high-skilled roles at a range of locations across the country.

RELX Comments

Introduction

1. RELX welcomes the opportunity to submit comments to this 'call for views'.

   We make our comments drawing on our expertise as a world-leading provider of data-driven solutions which help financial institutions and other organisations prevent crime and achieve regulatory compliance.

   We have therefore focused our comments in particular, though not exclusively, on suggesting approaches to conditions and derogations that will allow the UK to maintain and bolster efforts to ensure that it remains a jurisdiction in which financial institutions, companies and others can meet their due diligence obligations, assess risks and take reasonable steps to prevent, detect or investigate crimes.

2. Article 10 of the GDPR severely restricts the ability of service providers or companies to use information about criminal records *unless* a member state specifically authorises such uses. Similarly Article 9 restricts the use of information such as political affiliations or biometric data absent such country-specific authorisation. In particular, 9(2)(g) and 9(2)(j) allow member states to authorise the use of this type of information for any reason of substantial public interest, or for any archiving purpose in the public interest. These provisions were drafted to enable the use of exactly these types of personal data in order to bolster security, comply with legal obligations, prevent crime, and for other reasons in the public interest. Furthermore, the GDPR's recitals make it clear that such uses are important and expected but that they should be authorised country-by-country. For example, see GDPR Recital 19, which discusses examples including crime prevention and anti-money laundering data uses.

3. RELX therefore submits that the opportunity to introduce conditions in Articles 9 and 10 should be authorised so that such data uses – including use of sensitive data and criminal record data -- can continue as they exist today, helping to prevent crimes ranging from terrorism to fraud to identity theft. We suggest minor language changes to ensure such beneficial uses are not unintentionally narrowed (e.g., do not reference anti-fraud uses if the derogation really means "anti-crime" uses). We also understand that such uses would be subject to appropriate safeguards.

4. Furthermore, we propose that companies that create and offer diligence services that can be used for those purposes should explicitly be authorised to create and provide such services to the financial institutions, companies and other institutions that need them.

Examples of Data Uses to Serve the Public Interest and Meet Legal Obligations

5. It is clear that criminal record information and other sensitive data are a significant tool that companies use to effectively conduct due diligence or take other steps to comply with law. A non-exhaustive list of significant data use examples includes:

Activity	Observations
Anti-Money Laundering (AML) Compliance	• AML compliance requires financial institutions and others to know their customers and restrict the ability of criminals and terrorists among others to open accounts or launder funds. Criminal records are a necessary part of AML due diligence. • AML obligations also require institutions to understand when they are doing business with "Politically Exposed Persons" or "PEPs". This requires use of data about political affiliations.
Vendor Due Diligence	Many laws – including the GDPR itself – require firms to conduct due diligence before hiring vendors to handle various tasks such as caring for the infirm, handling personal data, or other important tasks. Those laws and good business practice requires firms to undertake diligence inquiries about their proposed vendors, including inquiries about their relevant criminal records.
Biometric Security Measures	Some firms bolster security by using fingerprint readers and other advanced devices to identify individuals, for example for internal information security or access control purposes. The importance of network information security is recognised at recital 49 of the GDPR. In addition to the Article 9 conditions and derogations described above, Article 88(1) also allows scope for member states to authorise these practices in an employment context.
Fraud/Crime Watch Lists	Fraud and crime watch lists are important tools that serve the public interest. For example, a number of firms identify specific IP addresses as representing a higher risk of fraud or crime based on past unlawful activities associated with the IP address (e.g., phishing attempts, identity theft, publicized fraud, etc.). The use of such lists is important to ensure that companies can escalate security measures where appropriate and prevent crime.

6. In each of these examples, firms use criminal record data or other sensitive data to meet critical legal obligations or to serve public interest needs.

7. Importantly, in the real world firms with a diligence or compliance need often do not create their *own* data set or watch list. Instead they use diligence, AML, PEP or watch list services created and kept up to date by firms with expertise in performing those functions in a high quality, accurate and well-documented manner. The use of data by such service firms is a key element in the global battle against crimes which are often attempted by increasingly sophisticated perpetrators. Certain RELX businesses offer such watch list and other services which is a key reason why we chose to submit these comments.

Scope of Needed Derogations

8. The Government has specific expertise in crafting appropriate legislative language such as the authorization of the conditions and derogations that these comments advocate. We write here to suggest that the wording not be kept too narrow to allow for legitimate processing to continue where it is necessary to prevent any crime (including fraud), as well as breaches of legislation / regulation, which may not necessarily attract a criminal sanction, but would otherwise be in the public interest.

9. For example, some existing conditions and derogations to current data protection law we would suggest have been drafted too narrowly. Condition 7A of Schedule 3 to the Data Protection Act 1998 (or 'DPA') permits the processing of sensitive personal data in certain cases related to "anti-fraud organisations". We respectfully believe that such data uses serve the public interest when used with respect to any crime, or breaches of legislation, not just fraud.

   Similarly, Data Protection Order 2000/417 allowed for processing sensitive personal data where the processing is:

   (i) in the substantial public interest, (ii) necessary for the purpose of the prevention or detection of any unlawful act or for the discharge of any function designed to protect the public against dishonesty, malpractice, or mismanagement of any person, and (iii) necessarily carried out without the explicit consent of the data subject being sought so as not to prejudice those purposes.

   It also contained important terms for the "insurance business". This derogation, although broader that Condition 7A, was still somewhat too narrow. For example it addresses the prevention or detection of unlawful acts but not necessarily the investigation or remediation of the unlawful acts. The Order also contains important terms for the "insurance business".

10. We propose that the GDPR conditions and derogations keep the existing DPA authorised conditions and derogations (to include those conditions contained within the supplementary Statutory Instruments) but also explicitly broaden the references to include other comparable matters. Even GDPR Recital 19 goes beyond the prevention and detection of crimes to: [Allow] "the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security."

11. Further, in reference to Articles 9(h) and (i), and, 89, we propose that the government seek to transpose across the protections afforded to personal data processing conducted in the interests

of research, and, statistics, whilst widening the scope to include analytical purposes where this purpose is not clearly defined in current legislative text. This is crucial for organisations such as ourselves as such processing purposes allows for product and research innovation, in particular in the areas of telematics, risk profiling, medical research and personal diagnosis.

12. Finally any derogation should also explicitly allow companies to create and provide services designed to help firms meet the array of purposes, which are authorised in the derogation legislation. This would serve the public interest by allowing institutions to use professional providers of such services, as they do today.

For further information, please contact: