ICO analysis of the Council of the European Union text of the General Data Protection Regulation

On June 15 the Council of the European Union finally agreed its version of the text of the General Data Protection Regulation. This is an important development in the life of the Regulation. It means that finally the EU's three main institutions – the Commission, the Parliament and now the Council – have all produced their own texts of the Regulation which form the basis of the trilogue process, which began recently. The agreed trilogue timetable aims to complete the process by the end of 2015. (See http://www.eppgroup.eu/news/Data-protection-reform-timetable

We thought it would be useful at this point to set out our observations on the parts of the Council text that we consider to be most in need of improvement during the trilogue process. We've indicated previously where we are supportive of the text and the benefits these changes will bring. As ever, our observations are based on our experience of regulating compliance with current data protection law. Our objective is to ensure future law provides effective protection for individuals whilst being easy to understand and working well in practice. We hope our comments will be of use to those involved in the legislative process.

Article 2a (Material scope)

We understand the need for Member States to be able to make their own national arrangements for data processing activities that fall outside the scope of the Regulation. In particular, we understand the need for flexibility in terms of the application of the Regulation to processing carried out by certain public authorities. We can also understand why some Member States want their own local arrangements in respect of the preservation of data protection arrangements that exceed current EU standards. We recognise that this has been a contentious issue during the Council negotiations. However, there is a danger of different data protection regimes developing. Any separate arrangements must be kept to a minimum and must follow the basic standards of the Regulation itself. In particular, the Data Protection Directive, which applies to competent authorities carrying out law enforcement functions, must be aligned as closely as possible with the Regulation.

Article 4 (Definitions)

Pseudonymisation: In our view there should be a single definition of 'personal data'. Therefore it is welcome that 'pseudonymous data' is no longer treated as a separate category of personal data. However, pseudonymisation should only be relevant as a privacy enhancing technique – for example in relation to data minimisation or security. It would be better not to try to define pseudonymisation in the context of the definition of personal data.

As it stands, the relevant Recital (23) is confusing. It says that pseudonymous data should be considered as information on an identifiable natural person – this implies all pseudonymous data whoever it is held by. However, the relevant Recital's new reference to the likelihood of identification presumably means that some pseudonymous data would be personal data whilst other pseudonymous data would not be, depending on the likelihood of the relevant identifying information being added to the pseudonymous information.

As it stands, the Article 4 definition seems to envisage pseudonymisation taking place within an organisation as part of a 'Chinese walls' arrangement. However, pseudonymisation is relevant more widely as a privacy enhancing technique, for example where pseudonymous data is disclosed from one organisation to another for research purposes.

We reiterate our view that if organisations are to go to the trouble of creating and using relatively low-risk forms of personal data – such as pseudonymous data – then the Regulation should provide some clear and proportionate incentives for doing so. This should be part of a wider risk based approach that should be developed further elsewhere in the text.

Article 6 (Lawfulness of processing)

Incompatible further processing: This part of the Article is a confusing conflation of legal bases for processing personal data and purpose limitation. The two elements of the law must be kept separate as far as is possible. Personal data processing must always have a legal basis and any incompatible processing that is allowed should be done within the terms of a relevant exemption from the data protection principles, in particular the purpose limitation requirement.

In practice, it would be difficult for an organisation to evaluate whether or not its legitimate interests override those of the individual and whether or not, therefore, the incompatible processing is permitted. Supervisory authorities would find this just as difficult to evaluate.

Article 7 (Conditions for consent)

Consent: One of the benefits of the approach to consent in the Commission's original text was the removal of the confusing distinction between 'consent' and 'explicit consent'. However, there is a danger that the references to 'explicit' or 'unambiguous' consent that appear here, in the Article 6 definition and elsewhere in the text will mean that – once again – organisations will be confused as to the type of consent they need to obtain in order to legitimise their processing of personal data in particular contexts. We believe that we need a single, high standard of consent and that should be either 'explicit', 'unambiguous' or both, but not one or the other depending on context. In reality, supervisory authorities are likely to focus on whether consent if of a sufficiently high standard in the round, not solely on whether it is 'explicit' or 'unambiguous'. We reiterate our view that there must be realistic alternatives to consent – for example 'legitimate interests' where the data processing is necessary to provide the goods or services that an individual has requested.

Article 8 (Child's consent)

We support the general idea of special protection for children in respect of the processing of personal data about them. However, this Article is too inflexible and will lead to uncertainty for those offering information services that are accessed by children. We note that 'child' is no longer defined, meaning that service providers will not know whether they need to obtain parental consent or not – even if they do know the age of those using its services – which in many cases they won't. The removal of the definition of 'child' also means that the Council text is unnecessarily more restrictive than the other texts, because the provision could apply to all children, not just those under 13.

We also believe that, provided they are offered in a clear and straightforward way with the necessary privacy protection in place, children should be able to access certain services without parental consent. This is part of a child's digital socialisation.

We have concerns that the introduction of an age-verification and parental consent system will lead to service providers collecting 'hard' identifiers in respect of children (and their parents) who may currently use their services anonymously or at least using relatively low-risk forms of identification. This would be a poor outcome in terms of personal privacy.

Article 12 (Transparent information, communication and modalities for exercising the rights of the individual)

The reference to providing information to individuals in clear and plain language is welcome. However, the Article is very much framed along the lines of the 'classical' privacy notice, but with more detail added. It fails to encourage organisations to find innovative ways of explaining their increasingly complex information systems to 'ordinary' people. We would like to see more encouragement for this.

In Article 12, 1a, we do not understand what organisations will be expected to do to demonstrate that they cannot identify someone, especially given the Regulation's wide definition of 'personal data'. There is illogicality here too in that if someone cannot be readily identified then no personal data about that person is being processed and so the individual's rights do not kick in.

Article 14 and 14a (Information to be provided where the data are collected from / have not been obtained from the individual)

The separation of these two articles is welcome, as it accentuates the differences between these two basic data collection scenarios. In particular, Article 14a gives a clear message to organisations obtaining personal data from sources such as data brokers that individual transparency obligations will normally still apply.

Article 15 (Rights of access for the individual)

This is a very important Article because subject access is the right most used by individuals. Many organisations – particularly SMEs - may have their only direct contact with the requirements of data protection law through dealing with subject access requests. Therefore the provisions relating to subject access must be as clear as possible in terms of what individuals are entitled to, the time limit for granting access and how much it costs.

The distinction between the right to access information for free (Article 15,1) and the right to obtain a copy of the personal data without excessive charge (Article 15, 1b) will be confusing. The right of access – as it is generally currently understood – means the right to obtain a copy of personal data.

We are not against a fixed but modest subject access fee, set on a national basis but we do not want to want to have to deal with disputes about whether the fees organisations charge are excessive or not. (We

know from our experience of FoI that disputes over disbursement - and costs generally - can be difficult to resolve.)

Article 15,2a is unacceptable in terms of data controllers not having to provide a copy of someone's personal data where this would involve the disclosure of another data subject's personal data. Does this mean, for example, that a hospital would not have to provide a copy of a patient's health record because it contains the personal data of the patient's doctor? The third party's personal data should only be withheld if, as is the case currently under UK law, the third party's right to privacy exceeds the data subject's right to access the information. We also note that this provision only applies when providing a copy of the data, but not when providing access to it – this seems illogical.

Article 17 (Right to erasure and to be forgotten)

We do not favour the term 'right to be forgotten' in the title of this Article. The use of the phrase is already leading individuals to believe they have an absolute right to the deletion of their data when this is in fact highly qualified and may be impossible to deliver in practice. We prefer just 'right to erasure'.

We welcome the reference to the right of freedom of expression and information in Article 17,3.

Article 19 (Right to object)

This is a key right that should not be watered down from the Commission's original proposal. However, it will be difficult for us to explain it to members of the public if the application of the right depends on the legal basis being used to legitimise the processing of the personal data. The complex matrix of rights and legal bases here, and in other parts of the Regulation, will lead to confusion for organisations and individuals. The two elements of the Regulation should be separated as far as is possible.

Article 20 (Automated individual decision making)

We support the reference to 'significantly affects' in this Article and the clarification that this test applies in respect of the right to object to profiling in, for example, a relatively low-risk context such as behavioural advertising. (Again the mixture of rights and legal bases for processing is problematic.)

Article 20, 1b implies that in certain circumstances – for example Where there is a contractual relationship between the two parties - data

controllers are always required to provide a 'human intervention safeguard' to the data subject. We do not believe that this is always possible, for example in behavioural advertising where online behaviour is analysed and particular content delivered. It is not clear what form of human intervention would be appropriate here. (We are not convinced that much online profiling has either a legal or a significant effect on the individual. If so this provision would not kick in anyway.)

The Commission's original text was more realistic in that the right to obtain human intervention was just one possible form of safeguard.

Article 28 (Records of categories of personal data processing activities)

We can understand why such a level of documentation might be appropriate for large, complex, information-based businesses. However it would be disproportionately burdensome for many businesses to be expected to keep such a detailed record of their data processing activities. This would be better addressed in scalable guidance from national supervisory authorities or EDPB, aimed at particular types of data controllers and data processing scenarios.

Article 31 (Notification of a personal data breach to the supervisory authority)

We are concerned about the possibility of receiving a large number of notifications of trivial or inconsequential data breaches. Therefore the reference to 'high-risk' breaches, and the illustrations of this, is welcome. The same considerations apply to Article 32 (informing the data subject directly).

Article 34 (Prior consultation)

It is welcome that organisations will not have to consult the supervisory authority where they have taken risk mitigation measures. Consultation with the supervisory authority should only be obligatory in exceptional circumstances if at all. We are therefore concerned that a failure to consult the supervisory authority falls within the highest tier of administrative fines – see Article 79a,3,de. This could have a perverse effect, meaning that data controllers err on the side of caution, consulting the supervisory authority too readily and diverting the supervisory authority's attention from genuinely risky processing.

Article 35 (Designation of the data protection officer)

Firstly, we support a requirement for organisations to have appropriate staff resources in place to comply with data protection law. What is appropriate would depend on the nature of the data processing that the organisation carried out and the risk it poses to individuals. This is consistent with the principle of accountability. We also recognise that different organisations have a different approach to compliance and that the single, independent data protection officer approach is just one model. Very often – especially in larger and more complex organisations - compliance is managed across cross-disciplinary teams and the Regulation must not be so tightly drafted as to discourage alternative approaches to compliance.

We presume that the amended wording of Article 35,1 means that the appointment of a data protection officer is not mandatory as it had been in earlier drafts of the Regulation, unless this is a requirement of EU or Member State law. This would mean that the appointment of a DPO could be mandatory in say Germany but not in the UK. This flexibility is welcome.

We appreciate that a data protection officer must have the necessary authority, skills and expertise. However, the list of qualities and functions in Articles 36 and 37 is excessive and unrealistic and does not reflect the way many organisations manage their data protection compliance.

Article 38 (Codes of conduct)

We still welcome the recognition of the significance of codes of conduct in developing a self-regulatory or co-regulatory approach to data protection compliance. The recognition that third parties – such as trade bodies – can oversee the operation of a code of conduct is particularly welcome, as is the reference to transfers of personal data to third countries in Article 38,1ab.

Article 51a (Competence of the lead supervisory authority)

The part of the Regulation dealing the competence of data protection supervisory authorities has become confusing and overly complex. It needs to be simplified. We maintain our view that local data protection issues should continue to be dealt with on a local basis – therefore we welcome the clarity of Article 51a, 2a. The lead authority should not have the option of 'calling in' a purely local case, as provided for in Article 51a, 2b. This seems particularly unnecessary as the 'local' authority can – and

probably will – produce its own draft decision anyway, of which the lead authority shall take 'utmost account'.

We note that 'lead authority' is not defined – unlike 'concerned authority', defined in Article 4, 19a. Although Recital 97 explains the role of the lead authority, we are concerned that in many cases it will not be clear which supervisory authority is the lead. This could be a particular problem where a company, or group of companies, has a number of substantive establishments across the EU. We need a clearer definition of 'lead authority', perhaps backed up with criteria for establishing this issued by EDPB.

Article 54a (Cooperation between the lead supervisory authority and other concerned supervisory authorities)

We maintain our view that lead supervisory authorities – with competence based on the location of the data controller's main establishment – should normally be able to regulate transnational processing without the formal involvement of other supervisory authorities or the EDPB. Therefore we believe that the lead supervisory authority's receipt of a relevant and reasoned objection is too low a threshold to trigger the consistency mechanism. A more evidential approach is needed, perhaps based on the likelihood of prejudice to individuals' interests if the lead authority's original decision is implemented. Otherwise, there is a danger of a large number of complaints being subjected to the consistency mechanism. It could mean – in reality – that complaints about the big transnational technology companies are always dealt with by EDPB rather than the data controller's lead supervisory authority. This should not be the outcome of the co-operation and consistency mechanism.

In general we find the relationship between the EDPB and national Member State courts uncertain. The Council's text appears to give the EDPB significant ability bind national courts and we are unsure how this will be effective and enforceable in practice. The legal standing of EDPB decisions and how these can be challenged – presumably in the CJEU – requires further consideration and clarification in the text.

Article 59 (Opinion by the Commission)

We support the deletion of this article, consistent with our view that as far as is possible matters should be resolved within the supervisory authority / EDPB community with minimal intervention from the Commission.

Article 66 (Tasks of the European Data Protection Board)

In Article 66,1(cb), supervisory authorities – or a third party working on their behalf - should be responsible for carrying out the accreditation of supervisory bodies on a national basis. EDPB should only have a role in relation to trans-national European schemes.

Article 79 (General conditions for imposing administrative fines)

The basic three-tier system linked to levels of fine lacks flexibility and space for the exercise of supervisory authority discretion. We are concerned that within this structure some administrative breaches that could be relatively minor – for example a failure to designate a 'representative' – fall within the highest sanction tier. On the other hand some breaches relating to basic individual rights fall within the lowest sanction tier. This does not reflect the adverse impact of the various types of breach on the privacy of individuals – this should be the determining factor. Our preferred approach would be to remove the three tiers and have a single list of breaches that can attract a fine.