ARTICLE 29 DATA PROTECTION WORKING PARTY

14/EN
WP 222

Statement on the results of the last JHA meeting

Adopted on 17 September 2014

Context

During the last Justice and Home Affairs (JHA) meeting (5 and 6 June), the EU Council reached a general approach on specific aspects of the draft data protection regulation.

This approach covered the following issues:

- the provisions on territorial scope Article 3(2);

- the definitions of Binding Corporate Rules and "international organisations" (Articles 4 (17) and (21); and

- the provisions on transfers of personal data to third countries or international organizations (Chapter V).

The WP29 welcomes this agreement as it constitutes an important step in the process towards an EU comprehensive framework on data protection. The WP29 would like to stress the importance of a range of options to enable transfers. However, it remains concerned regarding the impact on the resources of data protection authorities if the process regarding those new transfers' tools are not properly promoted or enabled. In the context of the forthcoming negotiations, the WP29 would like to share its views on this general approach.

1. Territorial Scope

The compromise text foresees that the Regulation applies to non-EU data controllers where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment by the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the European Union

Furthermore, Recital 20 provides additional specifications on determining whether such a controller is offering goods or services to data subjects in the Union. More specifically, these provisions go further by foreseeing the evaluation of whether the controller is envisaging doing business with data subjects residing in one or more Member States in the Union (e.g. use of language or a currency generally used in one or more Member States).

The WP29 welcomes these provisions as they not only clarify the territorial scope, but also underline the need to broadly ensure the application of EU rules on controllers that are processing personal data of EU data subjects but are not established in the EU. The text also reflects the WP29's views expressed in its previous opinion (WP191/opinion 01/2012).

Nevertheless, the WP29 would like to draw attention to the necessity for covering non-EU processors when the processing targets an EU citizen, as proposed by European Parliament (Article 3(1)).

2. Transfers of Personal Data to Third Countries or International Organizations (Chapter V)

Application of binding corporate rules

The article 43(1)(a) foreseen that "every member" of the group has to be bound by the BCR. The WP29 recommends that this should be "every relevant member" as not all entities within the group transfer data, or it can also be that not all entities within the group are intended to be part of the BCR.

Introducing new tools to frame transfers

The compromise text (Article 42(2)) dictates that transfers to third countries can take place, if the controller or the processor applies appropriate safeguards (i.e.: BCRs, standard contractual clauses, etc.). These safeguards can include codes of conduct and approved certification mechanisms as well as legally binding and enforceable instruments between public authorities or bodies.

The codes of conduct/approved certification mechanisms should contain binding and enforceable commitments taken on by the third country controller or processor to guarantee the protection of the personal data originating from the EU.

Moreover, there is a dichotomy established between the appropriate safeguards which do not require any specific authorisation from supervisory authorities (i.e.: BCR's, standard data protection clauses, legally binding instrument between public authorities, approved codes of conduct and certification mechanisms) and those appropriate safeguards which remain subject to authorisation from the competent supervisory authority (in particular, contractual clauses not based on agreed standard contractual clauses and administrative arrangements between public authorities).

1) Regarding the possibility to frame transfers by legally binding and enforceable instruments between public authorities or bodies

The WP29 welcomes this provision as it recognises not only the usual safeguards that are most likely to be used by the private sector (e.g.: BCRs, standard data protection clauses...) as well as the recourse to derogations for public sector transfers, but also the possibility to legally frame transfers between public authorities.

However, in some cases, the necessity of relying on arrangements which strive to be as legally and factually binding as possible—without formally being so—might be justified.

2) Regarding the possibility to frame transfers by codes of conduct or approved certification mechanism

The WP29 welcomes that codes of conduct or approved certification mechanisms contain binding and enforceable commitments by the controller or processor in the third country. Today, binding instruments are required for the governing of international transfers. With the existence of adequacy decisions, the availability of standard and ad-hoc contractual solutions and the new codification of binding corporate rules, it has become difficult to justify the need for basing transfers on non-binding instruments in the private sector. It would be contrary to the "Community acquis" to envisage appropriate safeguards that are not provided for within a legally binding instrument.

Additionally, the possibility to frame transfers with an approved certification mechanism or a code of conduct should be necessarily consistent with Articles 38 and 39 of the draft regulation and be framed by law.

As mentioned in a previous opinion, the Working Party is in favor of encouraging certification but calls for the inclusion of a better definition and description of the elements of the certification process.

Indeed, the WP29 considers that certification is a relevant tool to ensure compliance and to guarantee that internal privacy principles and procedures are implemented, efficient and reliable.

The WP29 believes that the scope of certification mechanisms for international transfers should be specified in order to clarify the interactions with other existing tools such as BCRs and contractual clauses.

The Working Party would furthermore like to reiterate that any certification scheme should not impact the supervisory role and the independence of data protection authorities. The following situation must be avoided: in the case of a data controller's or processor's non-compliance, the DPA shall first have to prove that this non-compliance stems from a deviation from the model that was certified before any other action may be considered. This would in many cases make enforcement very difficult, if not impossible.

Therefore, instead of certifying individual companies, the Working Party would prefer a mechanism for which data protection supervisory authorities and/or the EDPB provide guidance by setting the requirements and safeguards that certification schemes must meet to ensure compliance. Subsequently, the DPAs or the EDPB shall be strongly involved in the process of accreditation of the certification bodies.

Additionally, the criteria used to deliver accreditation to the certification body should be specified and could be based on existing requirements in other sectors (e.g.: environment, security, agriculture, health) or in international standards (ISO/IEC 17011). These criteria can include:

- Occupational competence: the certification body shall have a sufficient number of competent personnel (internal, external, temporary, or permanent, full time or part time) having the education, training, technical knowledge, skills and experience necessary for handling the work;

- Impartiality: the certification body shall be organized as to safeguard the objectivity and impartiality of its activities;

- Conflict of interest: the body must be free of actual or potential conflicts of interest;

- Confidentiality: it shall have adequate arrangements to guarantee the confidentiality of the information obtained; and

- Liability and financing: it shall have measures to cover liabilities arising from its activities and have sufficient financial resources.

In the case where the certification body incorrectly certifies the candidates, it should be subject to administrative pecuniary sanctions and to the withdrawal of its certification.

In order to ensure a genuine consistency and the same, high level of protection among all the implemented instruments, it is crucial that the same stakeholders define prerequisites for transfers (for BCRs, contractual clauses, codes and certification). Moreover, data protection supervisory authorities and the EDPB should be clearly involved in developing the referential to be used by certification bodies. The development of such a referential could involve the consultation of external stakeholders.

In any event, the same level of protection must be ensured whatever the instruments used (i.e., BCRs, standard contractual clauses, Safe Harbor, etc…) to avoid inconsistencies and breaches in the level of protection provided outside the EU.

The possibility to set limits on transfers in cases of important reasons of public interest

The text introduces an explicit provision authorizing the limiting of transfers of specific categories of personal data to third countries in cases of important reasons of public interest (Article 44(5)(a)). In that case, any national measures taken by the Member States shall be notified to the European Commission.

Given the revelations surrounding national security surveillance programs, the WP29 welcomes this provision.

However, the reference to the public interest concept may potentially be broadly interpreted (e.g.: does it cover the notion of national security?). Furthermore, this provision seems insufficient when ensuring a real and effective protection of European citizens. It therefore needs to be further clarified. The provisions foreseen in the European Parliament's new Article 43(a) could be useful in clarifying this notion.

In fact, in the proposed Article 43(a), the European Parliament introduced an obligation to inform individuals when a data controller has granted a third country public authority access to their data within the past 12 months as well as the obligation to obtain the authorization of the supervisory authority prior to the transfer. Being transparent about these practices will greatly enhance trust.

As mentioned in the Working Party's comments to the LIBE Committee's vote on 21 October 2013 (comments published on 11/12/2013), it was considered paramount that this proposal be accompanied by the conclusion of an international agreement, especially between the EU and the US in order to offer a robust and solid framework of protection. Therefore, when confronted with requests from third country public authorities for access, the competent supervisory authority should be the EU national authority dealing with the request rather than the data protection authority.

The maintained derogation for legitimate interests of the controller

Notwithstanding the transfers based on an adequacy decision issued by the Commission or appropriate safeguards (BCRs, contractual clauses, codes of conduct etc.) that are applicable to the public and private sectors, transfers can also be based on the derogations listed in Article 44. One of these derogations set out in Article 44(1)(h) allows for transfers based on legitimate interests pursued by the controller under the condition that:

- the transfer is not large scale or frequent;

- the legitimate interests of the controller may not be overridden by the rights and freedoms of the individual concerned; and

- the controller adduces suitable safeguards, as explained further in Recital 88.

The WP29 welcomes this provision as it is consistent with its position in previous papers (Opinion 1/2012 and Statement of 27 February 2013) affirming that such a derogation must be on an exceptional basis and only for non-massive non-repetitive and non-structural transfers.

The Working Party would once more like to stress that the binding force is one of the most important requirements for international transfer tools when ensuring appropriate safeguards for data subjects. Furthermore, self-assessment for transfers to third countries should—as derogation to adequate safeguards—remain very limited in scope.

In that respect, Recital 87 mentions the reduction and/or elimination of doping in sports as an important ground of public interest. The WP29 questions the opportunity to give such a special status to the fight against doping in sport, which in turn allows an international transfer to a third country without any further guarantees. Since the data at stake may be of a very sensitive nature, the WP29 is of the opinion that the transfer of such data should remain subject to the common principles applicable to all international transfers.