Council of the European Union

Brussels, 30 September 2015
(OR. en)

12524/15

Interinstitutional File:
2012/0011 (COD)

LIMITE

DATAPROTECT 153
JAI 700
MI 599
DIGIT 69
DAPIX 161
FREMP 198
COMIX 450
CODEC 1270

NOTE

From:	United Kingdom delegation
To:	Delegations
Subject:	Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Article 6(4)

Delegations will find in Annex a contribution of the UK delegation on Article 6(4) of the General Data Protection Regulation.

6.4. Where the purpose of further processing is ~~not~~ **in**compatible with the one for which the personal data have been collected **by the same controller**, the **further** processing must **be necessary for compliance with a legal obligation or necessary for reasons of public interest. This shall be on the basis of Union law, or Member State law which shall provide for appropriate measures to safeguard the legitimate interests of data subjects.** ~~have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract. **Further processing by the same controller for incompatible purposes on grounds of legitimate interests of that controller or a third party shall be lawful if these interests override the interests of the data subject.**~~

Issue

Businesses whose customers may have committed a crime must be able to disclose the customer's data to the appropriate authority. This might be done on request or pro-actively, e.g. the business discovers the customer is storing child pornography on its servers. As the personal data was collected for commercial purposes, the purpose of the disclosure may be deemed incompatible. Current EU law allows Member States to make provisions in their national law for such processing and other matters of public interest. It needs to be expressly permitted under the GDPR.

Proposal

In Council, there have been doubts expressed about Article 6.4. The UK therefore proposes a substantial restriction of this provision. This suggestion has a number of advantages:

- **Strict limitation:** narrowing A6.4 to processing necessary to fulfil a legal obligation or for the public interest prevents businesses from abusing A6.4 for purely commercial gain.
- **Protection of the data subject:** the redrafting stipulates that the processing must have a basis in law that contains suitable safeguards to protect data subjects' legitimate interests.
- **Reflects the status quo:** the redrafting is in compliance with the standard of protection set out in Directive 95/46/EC and required by the Charter of Fundamental Rights.
- **Permits essential processing:** the redrafting is targeted at permitting processing whose purpose is of value to our societies, in particular for defending the rights and freedoms of the most vulnerable.

Below, we firstly set out how the current legal framework provides for this essential processing, and how this is similar to our suggestion. Secondly, we set out why this essential processing may not be permitted under the Council or European Parliament's provisions of the GDPR. Particular reference is made to assessment of compatibility. Our proposal has no effect on what is to be deemed compatible under A6.3a. Instead, it provides legal certainty for controllers whose processing may be viewed as incompatible.

Status Quo – situation under current EU law

Such a revised clause meets the standard set by the provisions of Directive 95/46/EC and the Charter of Fundamental Rights (CFR).

- Article 6.1.b of the Directive introduces the purpose limitation principle. It states that *"personal data must be collected for specified, explicit, and legitimate purposes, and not further processed in a way incompatible with those purposes."* Article 13.1 then permits Member States to make exceptions in law to this principle. These exceptions must be to safeguard certain public interests, such as the prevention of crime and the collection of taxation, or to protect the rights and freedom of others[1].

- Article 8.2 of the CFR states that the data must be processed *"for specific purposes and on the basis of ... some other legitimate basis laid down by law."* While it does not reference the concept of further processing, the CFR stresses in Article 52 that any limitation on the rights and freedoms must be provided for by law and respect the essence of those rights and freedoms.

A restriction of Article 6.4 to only processing in compliance with a legal obligation or for the public interest conforms to both the above. This is reinforced by the requirement for the processing to have a base in law, containing suitable safeguards for the data subject.

[1] The UK, and several other Member States, have used this to make explicit exemptions in domestic law, such as for processing necessary for the prevention of crime. In the UK, S29.3 of the 1998 Act allows disclosures for the prevention of crime and the collection of taxation. S35 allows for disclosures in compliance with a legal obligation.

Situation under the GDPR

- Why Article 21 is not sufficient: Article 21 does allow Member States to make certain derogations to various provisions of the GDPR. But only the original text proposed by the European Commission permits such a derogation in domestic law to Article 5.1.b. This derogation is missing in both the Council and Parliament texts.

- Why Article 6.3a is not sufficient: Differing interpretations of compatibility make it hard to argue that our processing examples, for example a company passing information about one of its customers to law enforcement authorities due to concern about child protection, are compatible. A list of suggested factors for assessing compatibility is given by Article 6.3a. While the list is not exhaustive, it is still too narrow. It does not explicitly include whether the processing is based on a law and in the public interest.

  Legal certainty is vital, since companies who fear the GDPR's prospective sanction regime may be particularly risk-averse. All the processing examples in this paper carry a high risk of incompatibility, as indicated in current regulatory guidelines:

  Firstly, Opinion 2013/3 of the Article 29 Working Party sets out a key factor determining incompatibility. This is when the further processing would have a "significant potential impact" on the data subject. Such impact could encompass "criminal sanctions, arrests, and tax consequences". All these are likely consequences of the examples we give in this paper.

  Secondly, the Opinion also highlights the relationship between the original purposes of collection and the intended further purpose. Compatibility between purposes does not require identical processing. However, the gap between commercial purposes and law enforcement purposes is extremely wide.

  Thirdly, the Opinion notes that data subjects may not reasonably expect processing for such a different purpose. This is particularly true if they have not been under suspicion before.

The Opinion concludes that these three factors - a significant potential impact on the data subject, a lack of relationship between the purposes, and a lack of reasonable expectations - are strong indicators that the further processing is incompatible. It suggests that such processing should only be done under the strict conditions of Article 13.[2] As we have noted above, this would **not** be possible under the corresponding Article 21 of the GDPR.

In light of those three factors, many of the examples given in the annex pose a high risk of being judged incompatible. Some may be viewed as borderline. But all represent processing that is vital for society and which is vital to defend the defending the rights and freedoms of vulnerable persons. This factor is not taken into account in Article 6.3a.

- Why Recital 40 is not sufficient: Recital 40 states that indicating criminal threats could be a legitimate interest for the controller. However, this would apply to only to either new/initial processing, or to compatible further processing.

  The processing we envisage could not be considered "new" processing: it is still the same controller making the disclosure. The "new" processing would be done by the law enforcement authority after the disclosure is made. Such processing would then come under the draft Directive. The original commercial controller would have to start from scratch and re-collect the data for it to be considered truly new processing.

  Recital 40 may also pertain to compatible further processing, e.g. a criminal threat to the provision of the commercial service, such as fraud against it. It does not reference further incompatible processing. Even if it did, such a recital may not be sufficient to override the prohibition on further incompatible processing in the text in Article 5.1.b.

[2] Advice from the UK Information Commissioner's Office is similar. It considers a case when the police ask an employer for the home address of an employee under suspicion. As the address was collected for employment purposes and is disclosed for law enforcement purposes, this would be incompatible processing. The employer is advised to use the s29.3 exemption in the DPA 1998 in accordance with A13 of Directive 95/46/EC.
ICO Guidelines: Using the crime and taxation exemptions PP13-15
https://ico.org.uk/media/for-organisations/documents/1594/section-29.pdf

Conclusion

This paper presents a suggested amendment to limit the use of Article 6.4. The paper firstly set out how the amendment resembles the status quo. It showed how the redraft conforms to the standard of protection and the purpose limitation principle in Directive 95/46/EC and the Charter.

The paper secondly set out how existing provisions in the GDPR would be insufficient to accommodate the type of further processing envisaged here. Such processing would be unable to rely on the concept of compatibility to be legally valid.

Thirdly, an annex to this paper sets out the types of further processing that is legal under Directive 95/46/EC and must be preserved. All examples are of processing with a high or borderline risk of being deemed incompatible. All examples also reflect a purpose or goal that is of value to our societies. Many examples concern the protection of children from trafficking, rape, or abuse.

This processing must be allowed to continue. **A revised and restricted Article 6.4 is vital and the only legally certain means of permitting the processing**. The UK would welcome the opinions of other Member States on this suggested compromise.

Examples of Processing

In view of the above analysis, this paper lists a range of important further processing that is permitted under the current legal framework and must continue. Below are general examples which may be caught by the loss of Article 6.4 of the General Data Protection Regulation. Although the examples represent a very wide and diverse range of processing, there are four traits common to all:

- **Each example constitutes a case of further processing.** The personal data in each example were collected originally for a specific purpose. The data are then subsequently used for a different purpose.

- **Each example contains doubt about whether the further processing is compatible with the original purpose.** In many of the examples, the risk of the further purpose being deemed incompatible is very high.

- **Each example reflects a purpose or goal that is of value to our societies or is necessary to defend the rights and freedoms of others.** Many examples touch on the protection of children from trafficking, rape, and abuse. Other examples reflect the need to safeguard individuals through preventing crime and fraud.

- **Each example is case-specific.** No example entitles the controller to conduct further incompatible processing in all cases. Controllers must assess the individual circumstances and weigh up the different interests, which may include the public interest and their own legitimate interest. They must also consider what safeguards could and should be added. There should be no question of giving data controllers a blank cheque to further process personal data.

1. **Fighting against FGM**

   During a medical check up, a doctor discovers that one of her patients, a child, has recently undergone Female Genital Mutilation. As FGM is a criminal offence, she discloses the child's medical file to the police.

   Original purpose: Provision of health care

   Further purpose: Law enforcement/prosecuting gender-based violence

2. **Child Abuse**

   A vulnerable child goes missing. The police believe she may have been in contact with a man on an online social network who is exploiting her. Upon request, the social network discloses the child's personal data, including her list of 'friends' so that the police can find her and protect her from further abuse.

   Original purpose: Commercial

   Further purpose: Child protection/law enforcement

3. **Child Pornography**

   A online file storage company collects its customers' personal data, like names, address, credit card details in order to bill them for storage. In a routine security check, it discovers that a customer is storing files containing child pornography on its servers. The company sends the customer's personal information to the police.

   Original purpose: Commercial, providing a service

   Further purpose: Child protection/law enforcement

4. **Child Trafficking**

   A hotel chain processes the personal data of its guests for the purpose of providing its service. The police are investigating a child trafficking ring. Upon request, the hotel discloses information about a suspect who has stayed at the hotel and any children linked to his booking.

   Original purpose: Commercial

   Further purpose: Child protection/law enforcement

5. **Domestic Gender Based Violence**

A domestic violence victim is receiving abusive and threatening phone calls from her ex-partner. The telecoms company, on request, discloses the personal data they have on the ex-partner to the police, which proves that he made the calls near her property. This helps to lead to a successful conviction and helps to safeguard the victim and other potential victims.

Original purpose: Commercial

Further purpose: Preventing gender based violence/law enforcement

6. **Warm Homes for Pensioners**

An energy company processes the personal data of their customers for billing and commercial purposes. On request from the Department of Work and Pensions, the energy company discloses the personal data of certain customers who are pensioners and may be at risk of fuel poverty. The Department cross-checks this with their own datasets and awards a rebate to the eligible pensioners to help them afford heating costs.

Original purpose: Billing/commercial

Further purpose: Social care/combating fuel poverty for the most vulnerable

7. **Fighting against insider trading**

A financial advisor processes her clients' personal data for the purposes of recommending good investment opportunities. The advisor has reasonable grounds to suspect one of her clients is engaging in insider trading. She discloses the personal data and information about the suspicious transaction to the Financial Conduct Authority.

Original Purpose: Providing a service/commercial

Further purpose: Preventing market abuse/law enforcement

8. **Smart meters and crime**

An energy company installs smart meters in customers' homes. The purposes of processing involve ensuring energy efficiency. The police have reasonable grounds to suspect one of the company's customers of running a cannabis factory in their home. Upon request, the company discloses the customer's energy usage data to the police.

Original Purpose: Providing a service/energy efficiency

Further purpose: Law enforcement