17.

Comments about the Guidelines of The Article 29 Data Protection Working Party related to the right of data portability and WP242 ANNEX

The Guidelines of The Article 29 Data Protection Working Party around new rights and new requirements are absolutely necessary for all those organizations processing personal data and who wants to do so with strict subjection to the rules of application; by this same, the guidelines are particularly welcome by entities such as CaixaBank.

Through this document, we would like to give some comments, as well as to share certain doubts and concerns regarding the new right of portability, from a practical perspective (i.e. doubts and difficulties that we observe to apply and comply scrupulously in daily practice with the proposed guidelines).

We hope it is useful and please do not hesitate to contact us for any clarification you may need.

1. ABOUT THE CONDITIONS OF APPLICATION OF THE RIGHT OF PORTABILITY

As indicated on page 3 of the Guidelines:

This right applies data subjects to certains conditions

These conditions, in accordance with content of the guidelines, are the following:

(i) Personal data (anonymous data or data which does not concern the data subjecte will not be in scope)
(ii) Data carried out by automatic means (does not cover paper files)
(iii) Processing operations must be based (i) on the data subject's consent or (ii) on a contract to which the data subject is a party

COMMENTS

We understand (since the WP242 ANNEX is not conclusive on this concrete issue) that the conditions under which must apply the new right are exclusively those listed and not others; the conditions should be listed to avoid any interpretation.

2. ABOUT THE DIFFERENCES BETWEEN THE PORTABILITY RIGHT AND THE ACCESS RIGHT

As indicate on page 3 and page 11 of the Guidelines:

The right of portability is closely related to but differs from the right of Access in many ways

WP29 recommends in particular that data controllers clearly explain the difference between the types of the data that a data subject can receive using the portability right or the access right

COMMENTS

We need some help to explain clearly the differences mentioned, as is requires, because there isn't any experience in relation to the exercise of new right, so we would highly recommend the publication of a guide in this regard (difference between the types of the data that a subject can receiving using the portability right or the access right), useful for both data subjects and controllers.

3. ABOUT THE DIFFICULTY OF THE "THIRD PARTIES" TO CONTROL THEIR DATA

As indicated on page 3 of the Guidelines:

The new right to data portability aims at empowering data subjects

This right also represents an opportunity to re-balance the relationship between data subject s and data controllers, trough the affirmation of individual's personal rights and control over the personal data concerning them

This right offers an easy way for data subjects to manage and reuse personal data themselves

and

as indicated on page 7 and 8:

Any data which does not concern the data subject will not be in scope

but

as indicated on page 7:

Related to processing information that contains data of several data subject, controller must not take an overly restrictive interpretation of the sentence "personal data concerning the data subject"

and

as indicated on page 8:

The new controller should not process the receiving data for any purpose which would a

adversely affect the rights and freedoms of the third-parties

4. ABOUT THE LAWFULNESS OF PROCESSING OF DATA OF "THIRD PARTIES"

As indicated on page 9 of the Guidelines:

The data subject initiating the transmission of his or her data to another data controller, either gives consent to the new data controller for processing or enters into a contract with them.

Where personal data of third parties are included in the data set, another ground for lawfulness of processing must be identified (for example, a legitimate interest pursued of the new data controller)

COMMENTS

It could be understood that there is a difference of rights between data owners (between the data subject using his/her right of portability and the "third parties" which personal data are in the scope of the right of portability used), because the "third parties" do not enjoy the same control over their data or the aimed emporwerment them: the "third parties" depend on a decision of the data subject who, using his/her right of portability, decides on data of the "third parties" (transmission of his/her data *and, in may cases,* transmission of data of other subjects to a new controller).

Once this decision (transmission of the data to a new controller) has been taken by the data subject, all responsabilities (in relation to "third parties" data) are transferred, paradoxically, to the new controller, who

a. must use them for the same purposes
b. without infringing the rights and freedoms of the "third parties"

Regarding the letter a. (use of the data of "third parties" for the same purposes) it seems inevitable to question what guarantees or controls have or can be demanded by the "third parties" in relation to the requirement that their data would be effectively used for the same purposes (for the new controller or for the data subject).

Regarding the letter b. (without infringing the rights and freedoms of the "third parties"), any discrepancy in this point by the concerned "third parties" will result in the filing of complaints with a supervisory authority or in a judicial proceedings.

In addition, it doesn't seem very coherent that the right of portability is based on the consent or on a contract and, on the contrary, that the authorization to transmit the data of the "third parties" (unaware of such processing of their data) has another basis: the legitimate interest (when the portability right doesn't apply to processing operations based on the legitimate interest!).

The processing of the "third parties" data (who have not provided consent or which are not part of the contract) on the basis of a legitimate interest is a high risk (claims and complaints) for the controllers (still using them for the same purposes).

5. ABOUT THE REQUIREMENTS FOR THE CONTROLLERS TO PROCESSING THE DATA OF "THIRD PARTIES"

As indicated on page 10 of the Guidelines:

Controllers should implement tools to enable data subjects to select the relevant data and exclude (where relevant) other data subjects' data. Additionally, they should implement consent mechanisms for other data subjects involved (...)

COMMENTS

Regarding to these requirements, important technical developments are being demanded to the entities whose cost and implementation can be relevant and really difficult.

In addition, there is no definition of relevant data, and, by way of example, it is not feasible to seed consent from third parties in the case of a history of a data subject's bank account (e.g., obtaining the consent of all those who have transferred money to the data subject).

Finally, this requirements must also be required of data subject (reuse of the data) and Third Trusted Parties.

6. ABOUT THE SELFUSE / REUSE FOR DATA SUBJECTS

As indicated on page 4 of the Guidelines:

This right offers an easy way for data subjects to manage and reuse personal data themselves

COMMENTS

It seems to us that if the data to be used by the data subjects incorporates data of "third parties" (e.g., a contact list or, in a bank account, the names of all those have transferred money to the data subject), the same requirements as the controllers must be demanded (use of them for the same purposes and without infringing the rights and freedoms of the "third parties"), in order to avoid any injury to the rights of the "third parties".

For this same reason, we believe it is necessary to strenghten the indication that the data are *only for purely personal or household activity*, and recommend, as a good practice, that this indication will be incorporated in the transmission of the data carried out by the controller.

Finally, in the case where data subject transmits his/her data to a new controller (from his/her own devices), it would seem necessary to require that such transmission be made under the same requeriments as the controllers: (i) exclusion of relevant data of the "third parties" and (ii) mechanisms to obtain the consent of these "third parties"

7. ABOUT THE STORE IN PRIVATE DEVICES

As indicated on page 15 of Guidelines:

The data controller is responsible for taking all the security measures needed to ensure that personal data is securely transmitted (e.g. by use of encryption) to the right destination (e.g. by use of additional authentication information)

How to help users in securing ther storage of their personal data in their own systems?There is always also the risk that users may store them in a less secured system that the one provided by the service.

(i)The data subject should be made aware of this in order to take steps to protect the information they have recived

(ii) The data controller could also, as a best practice, recommend appropriate format(s) and encryption measures to help the data subject to achieve this goal.

and

as indicated on page 12 of Guidelines

If the size of data requested by the data subject makes transmission via the internet problematic (...) the data controller may also need to consider alternative means of providing the data such as using streaming or saving to a CD, DVD or other physical media

COMMENTS

It seems to us that it makes no sense that GDPR requires the adoption of important security measures to the controllers (or processors) to protect and ensure the confidentiality of data and there is no requeriments, only recomendations, for the data subjects storing personal data in their devices (containing their data and the data of the "third parties"), regardless of whether the controller is not responsible for the data once transmitted.

8. ABOUT THE STORAGE OF DATA BY A TRUSTED THIRD PARTY

As indicated on page 2 of the Guidelines:

Data portability can promote the controlled sharing of personal data between organizations and thus enrich services and customer experiences

and on page 5:

Data subjects may also wish use of a personal data store or a trusted third party

and on page 6:

(between organizations) *A receiving data controller is responsible for ensuring that the portable data provided are relevant and not excessive with regard to the new data processing*

(between organizations) *The new data controller must clearly and directly state the purpose of the new processing before any request for transmission of the portable data*

COMMENTS

The access of the controllers to the data stored by a Trusted Third Party (TTP) must be regulated in detail, and the same requirements should be demanded that in the case of transmission of data between two controllers (so, the TTP must check the purpose of the new processing, must transmit only data relevant and not excessive with regard to the new data processing, must comply with the security measures needed (storage and transmission), and, in the case of data of third parties, must check that the new processing is for the same purposes and doesn't infringe rights and freedoms of third parties).

9. ABOUT THE SENTENCE *"THE TERM PROVIDED BY THE DATA SUBJECTE" MUST BE INTERPRETED BROADLY, AND ONLY TO EXCLUDED "INFERRED DATA" AND "DERIVED DATA"*

COMMENTS

There are obvious practical difficulties in differentiating between

(i) OBSERVATION OF AN INDIVIDUAL'S BEHAVIOUR (*data provided*)
(ii) ANALYSIS OF THAT BEHAVIOUR (*data inferred/derived*)

For example, in the case of a financial service categorizing expenses (education, food, automotive, leisure,...), although these are *observed* data (provided by the data subject by virtue of the use of the service), in turn, they have been the object of an analysis to categorize them to be able to provide the requested service to the client.

For us, these data will not be within scope of the right of portability, but we don't have absolute certainty about it.

So, in many cases the line between observed data and inferred data can certainly be fine and the broad of definitions (and the lack of a significant number of concrete examples) may imply differences of interpretation that entail the filing of claims and lawsuits by the data subjects.

10. ABOUT IP RIGHTS

As indicated on the page 10 of the Guidelines:

A potential business risk cannot, however, in and of itself serve as the basis of a refusal to answer the portability request.

Data controllers can transfer the personal data provided by data subjects in a form that does not release information covered by trade secrets or intellectual property and trade secrets

COMMENTS

The observation capabilities of a tool, a software, an application, or a device (which will provide *observed data* -i.e. within the scope of portability-) may involve the disclosure of trade secrets or intellectual property rights.

The Guidelines are not realistic in relation to the trade secrets or intellectual property rights, essential assets for companies: this aspect must be developed with care and detail, to avoid legal uncertainties and arbitrary interpretations, that can have a huge impact and economic damage on organizations.

11. ABOUT THE TECHNICAL DEVELOPMENTS REQUIRED

As indicated on page and page 14 of the Guidelines:

WP29 encourages cooperation between industry stakeholders and trade associations to work together on a common set of interoperable standards and formats to deliver the right of portability

COMMENTS

An encouragement is not sufficient, but an urgent european initiative is needed to study, address and give solution in the short term, since the technical requirements will be demandable in little more than a year.

12. ABOUT THE FEE (IN CASE OF MULTIPLE DATA PORTABILITY REQUESTS)

As indicated on the page 12 of the Guidelines:

(...) the answering of multiple data portability request should generally be considered to impose a excessive burden

COMMENTS

More detail or direction are needed regarding to the amount of the fee (a range of applicable amounts, or objective quantification elements).

CAIXABANK, S.A.

Innovation and Privacy Legal Department

February 2017