

BRE-JBZ

From: Kaai, Geran
Sent: vrijdag 3 april 2015 15:56
To: Verweij, Ellen
Subject: FW: Data Protection Reform
Attachments: BEUC-L-2014-173 mgo Letter to Ambassadors_Perm Reps.pdf

From: BRE-CDP
Sent: dinsdag 3 juni 2014 17:42
To: Kaai, Geran; Luijsterburg, Sander
Subject: FW: Data Protection Reform

From: BEUC - Legal-Eco [mailto: [REDACTED]]
Sent: dinsdag 3 juni 2014 17:38
Cc: BEUC - Digital
Subject: Data Protection Reform



Permanent Representation to the EU

The Consumer Voice in Europe

Ref.: BEUC-L-2014-173/MGO/KRO/rs

3 June 2014

Re: Data Protection Reform

Dear Ambassador,

I write on behalf of the European Consumer Organisation (BEUC) to draw your attention to a number of outstanding issues in light of the ongoing negotiations on the data protection reform package and urge you to reach an agreement in Council on the draft proposal as a matter of urgency.

Over the last two years, the Council has made significant progress at technical level. Now, political commitment is needed to transform the extensive work into real progress. It is important to reach a political agreement rapidly that allows the adoption of the new rules by the end of 2014, as requested by the European Council.

The adoption of the Data Protection Regulation is a major component of the EU Digital Agenda. A robust data protection legal framework would help boost consumer confidence and provide businesses with a coherent and comprehensive legal framework across Europe. The objective of the reform is to strengthen existing rights

and principles while restoring consumer control over the way their personal data is processed. The right to the protection of personal data should not be eroded or undermined simply because it has become easier or more profitable to breach it in the digital environment.

The proposal for a Data Protection Regulation strikes the correct balance between the need for an effective system of data protection for EU consumers and citizens against not confronting businesses with excessive administrative burden. The reform will generate growth because it will modernise the legal framework and facilitate the use of data protection rules across Europe.

We note the progress achieved under the Greek Presidency. However, we regret that compromise solutions have not yet been found on important issues. Of even greater concern, it appears the existing *acquis* might be weakened in some respects.

In view of the ongoing discussions, we would like to reiterate the position of BEUC on a number of crucial issues.

Scope of the General Data Protection Regulation: need to include the public sector

BEUC is opposed to the exclusion of the public sector from the scope of the Data Protection Regulation. Such an exception would lower the level of protection in Directive 95/46 which does not distinguish between the public and private sectors. The public sector already benefits from provisions which allow the processing of personal data when necessary in order to comply with a legal obligation, or for tasks performed in the public interest. Furthermore, the lines between the public and the private are blurring, with the same type of activities being performed by public bodies in some Member States and by private entities in others.

Need for a broad and flexible definition of personal data

The definition of personal data is crucial in defining the scope of the draft Regulation. In an interconnected digital world, individual pieces of data cannot be regarded in isolation. In order to ensure the new data protection rules remain relevant in years to come, the definition of personal data should remain broad and flexible in light of the rapidity of ICT developments.

Re-identification and 'de-anonymisation' of personal data are increasingly common malpractices. Full anonymisation is an illusion and increasingly difficult to achieve with the advance of computer technology and the availability of vast amounts of information.

When personal data is irreversibly anonymised, it automatically falls outside the scope of the Regulation. A definition of "anonymous data" should be avoided, as such a definition would increase the risk of loopholes. Such flaws could then be exploited by controllers to circumvent the rules of the Regulation.

With regard to pseudonymised data, we wish to stress that such data is, by definition, personal data as it relates to an identifiable individual and therefore falls within the scope of the draft Regulation.

Purpose limitation and data minimisation are crucial pillars of a sound data protection framework

The principle of purpose limitation is one of the crucial pillars of the data protection legislation. The data controller has the sole obligation to collect and process the personal data for specified, explicit and legitimate purposes, which are to be communicated to the data subject.

Further processing of data for purposes different to the original is only allowed if the new purposes are compatible with the original ones. However the notion of compatibility is not defined in the proposal. It is thus important that certain general criteria are put forward to be used to assess the compatibility of further processing.

BEUC proposes that the task of setting such criteria be entrusted to the European Data Protection Board. The recent Opinion by the Article 29 Data Protection Working Party already provides a basis:

- the relationship between the original purpose and the purposes of further processing;
- the context in which the data were collected; the reasonable expectations of the data subject;
- the nature of the data and the impact of further processing on the data subject;
- the safeguards applied by the controller to prevent any undue impact on the data subject.

Furthermore, should the data controller use and process personal data for purposes other than those originally foreseen without informing the data subject, consumers will lose control of how and when their data is processed and the entire system of protection will become opaque, weak and unstable.

Legitimate interests: need to prevent abuses

The legitimate interests of the data controller are possible grounds for lawful processing. However, companies have used this as a basis for the unrestricted and unregulated processing of personal data and not allowing user control.

Many companies use the 'legitimate interests' provision to collect more data than is required for the specified purposes - often for different purposes incompatible to the original. The legitimate interests ground is often used as a pretext to pass on data to third parties and evade compliance with data protection principles.

Therefore, unless properly defined and used only exceptionally, the legitimate interests of the controller will become the loophole of the new Regulation. Therefore we propose to provide the following:

- If a data controller wishes to use 'legitimate interests' as a basis for processing, this must be flagged to the data subject;
- The legitimate interests ground can only be used as a last resort i.e. when no other legal grounds are available;
- The data controller should prove that its interests override those of the data subject;
- The European Data Protection Board should be entrusted with the task of publishing an indicative list of processing operations which can be based on the legitimate interests of companies.

Consumer redress: need to maintain the provisions relating to group actions

When data protection rules are infringed or personal data protections breached, data subjects should be able to seek redress and effectively be compensated for the damage they suffer. For this to be feasible it is crucial that consumer organisations or associations defending their rights can lodge complaints or seek actions in court on behalf of a group of consumers.


Often the value of the damage caused to an individual is not worth a lengthy and expensive legal action. By putting Collective Legal Actions in place, it will be easier and less cumbersome for consumers to access redress and due compensated for the damage they have suffered.

The rights of organisations or associations defending data subjects' rights to lodge complaints before a supervisory authority (Article 73) and to bring an action to court on behalf of data subjects (Article 76) should be maintained.

The right of organisations to bring judicial actions for compensation should be added in Article 77.

We remain at your disposal to provide further information on the issues referred to above, as well as the other elements under discussion.

Yours sincerely,


Director General

The Consumer Voice in Europe

Ref.: BEUC-L-2014-173/MGO/KRO/rs

3 June 2014

Re: Data Protection Reform

Dear Ambassador,

I write on behalf of the European Consumer Organisation (BEUC) to draw your attention to a number of outstanding issues in light of the ongoing negotiations on the data protection reform package and urge you to reach an agreement in Council on the draft proposal as a matter of urgency.

Over the last two years, the Council has made significant progress at technical level. Now, political commitment is needed to transform the extensive work into real progress. It is important to reach a political agreement rapidly that allows the adoption of the new rules by the end of 2014, as requested by the European Council.

The adoption of the Data Protection Regulation is a major component of the EU Digital Agenda. A robust data protection legal framework would help boost consumer confidence and provide businesses with a coherent and comprehensive legal framework across Europe. The objective of the reform is to strengthen existing rights and principles while restoring consumer control over the way their personal data is processed. The right to the protection of personal data should not be eroded or undermined simply because it has become easier or more profitable to breach it in the digital environment.

The proposal for a Data Protection Regulation strikes the correct balance between the need for an effective system of data protection for EU consumers and citizens against not confronting businesses with excessive administrative burden. The reform will generate growth because it will modernise the legal framework and facilitate the use of data protection rules across Europe.

We note the progress achieved under the Greek Presidency. However, we regret that compromise solutions have not yet been found on important issues. Of even greater concern, it appears the existing *acquis* might be weakened in some respects.

In view of the ongoing discussions, we would like to reiterate the position of BEUC on a number of crucial issues.

.../...

Scope of the General Data Protection Regulation: need to include the public sector

BEUC is opposed to the exclusion of the public sector from the scope of the Data Protection Regulation. Such an exception would lower the level of protection in Directive 95/46 which does not distinguish between the public and private sectors. The public sector already benefits from provisions which allow the processing of personal data when necessary in order to comply with a legal obligation, or for tasks performed in the public interest. Furthermore, the lines between the public and the private are blurring, with the same type of activities being performed by public bodies in some Member States and by private entities in others.

Need for a broad and flexible definition of personal data

The definition of personal data is crucial in defining the scope of the draft Regulation. In an interconnected digital world, individual pieces of data cannot be regarded in isolation. In order to ensure the new data protection rules remain relevant in years to come, the definition of personal data should remain broad and flexible in light of the rapidity of ICT developments.

Re-identification and 'de-anonymisation' of personal data are increasingly common malpractices. Full anonymisation is an illusion and increasingly difficult to achieve with the advance of computer technology and the availability of vast amounts of information.

When personal data is irreversibly anonymised, it automatically falls outside the scope of the Regulation. A definition of "anonymous data" should be avoided, as such a definition would increase the risk of loopholes. Such flaws could then be exploited by controllers to circumvent the rules of the Regulation.

With regard to pseudonymised data, we wish to stress that such data is, by definition, personal data as it relates to an identifiable individual and therefore falls within the scope of the draft Regulation.

Purpose limitation and data minimisation are crucial pillars of a sound data protection framework

The principle of purpose limitation is one of the crucial pillars of the data protection legislation. The data controller has the sole obligation to collect and process the personal data for specified, explicit and legitimate purposes, which are to be communicated to the data subject.

Further processing of data for purposes different to the original is only allowed if the new purposes are compatible with the original ones. However the notion of compatibility is not defined in the proposal. It is thus important that certain general criteria are put forward to be used to assess the compatibility of further processing.

BEUC proposes that the task of setting such criteria be entrusted to the European Data Protection Board. The recent Opinion by the Article 29 Data Protection Working Party already provides a basis:

- the relationship between the original purpose and the purposes of further processing;
- the context in which the data were collected; the reasonable expectations of the data subject;
- the nature of the data and the impact of further processing on the data subject;
- the safeguards applied by the controller to prevent any undue impact on the data subject.

.../...

Furthermore, should the data controller use and process personal data for purposes other than those originally foreseen without informing the data subject, consumers will lose control of how and when their data is processed and the entire system of protection will become opaque, weak and unstable.

Legitimate interests: need to prevent abuses

The legitimate interests of the data controller are possible grounds for lawful processing. However, companies have used this as a basis for the unrestricted and unregulated processing of personal data and not allowing user control.

Many companies use the 'legitimate interests' provision to collect more data than is required for the specified purposes - often for different purposes incompatible to the original. The legitimate interests ground is often used as a pretext to pass on data to third parties and evade compliance with data protection principles.

Therefore, unless properly defined and used only exceptionally, the legitimate interests of the controller will become the loophole of the new Regulation. Therefore we propose to provide the following:

- If a data controller wishes to use 'legitimate interests' as a basis for processing, this must be flagged to the data subject;
- The legitimate interests ground can only be used as a last resort i.e. when no other legal grounds are available;
- The data controller should prove that its interests override those of the data subject;
- The European Data Protection Board should be entrusted with the task of publishing an indicative list of processing operations which can be based on the legitimate interests of companies.

Consumer redress: need to maintain the provisions relating to group actions

When data protection rules are infringed or personal data protections breached, data subjects should be able to seek redress and effectively be compensated for the damage they suffer. For this to be feasible it is crucial that consumer organisations or associations defending their rights can lodge complaints or seek actions in court on behalf of a group of consumers.

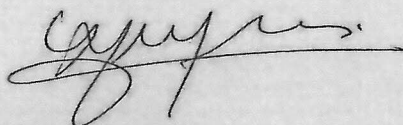
Often the value of the damage caused to an individual is not worth a lengthy and expensive legal action. By putting Collective Legal Actions in place, it will be easier and less cumbersome for consumers to access redress and due compensated for the damage they have suffered.


The rights of organisations or associations defending data subjects' rights to lodge complaints before a supervisory authority (Article 73) and to bring an action to court on behalf of data subjects (Article 76) should be maintained.

The right of organisations to bring judicial actions for compensation should be added in Article 77.

We remain at your disposal to provide further information on the issues referred to above, as well as the other elements under discussion.

Yours sincerely,




Director General