## ITEM C.1 EU-U.S. PRIVACY SHIELD

### Background

During its last Plenary meeting on 12-13 April 2016, the Working Party adopted its opinion on the draft adequacy decision and annexes constituting the EU-U.S. Privacy Shield package (hereinafter: Privacy Shield), which seeks to replace the previous U.S. Safe Harbour invalidated by the Court of Justice of the European Union on 6 October 2015, in the Schrems case.

This opinion contains the Working Party's assessment of the Privacy Shield in the light of the applicable EU data protection legal framework as set out in Directive 95/46/EC, as well as the fundamental rights to private life and data protection as enshrined in Article 8 of the European Convention on Human Rights and Articles 7 and 8 of the Charter of Fundamental rights of the European Union.

Its main goal was to check whether an essentially equivalent level of protection is maintained when personal data is processed subject to the provisions of the Privacy Shield.

### Conclusions of the opinion 01/2016 on the EU-US Privacy Shield draft adequacy decision

As starting general remarks, the WP29 underlined an overall lack of clarity of the Privacy Shield package, and recalled the need to be consistent with the EU data protection legal framework, both in scope and terminology, especially as the General Data Protection Regulation will enter into application in 2018.

Overall, the Working Party has welcomed significant improvements in the Privacy Shield compared to the Safe Harbour decision.

However, the Working Party has also expressed strong concerns on both the commercial aspects and the access by public authorities to data transferred under the Privacy Shield.

Regarding the commercial aspects, the main points of concerns were the absence or inadequate substitution of key data protection principles, the insufficient guarantees framing onward transfers, the complexity of the new redress mechanism.

Regarding access by public authorities to data transferred under the Privacy Shield, the WP29 also expressed concerns regarding the maintained possibility of bulk collection and the lack of independence and powers of the Ombudsperson.

### State of Play

The European Commission will give an update of the state of play in Plenary.

### Next steps: Discussion points as identified by ITS and BTLE subgroups

The following arbitration points have been discussed during the Future of Privacy (FoP) meeting on 24 May 2016:

REGARDING POSSIBLE ACTIONS **BEFORE** ADOPTION OF THE PRIVACY SHIELD ADEQUACY DECISION (*if possible as the timeline of the EC for adoption looks very tight)

The FOP subgroup suggested that no other opinion is adopted on the Privacy Shield nor any public statement whatsoever until the adequacy decision is finalized by the Commission.

Accordingly, it is not envisaged to send drafting proposals on the Privacy Shield to the EU Commission/Article 31 Committee.

Regarding access by public authorities to data transferred under the privacy shield, the BTLE also proposed to **wait and see the outcome** of the new negotiations engaged by the Commission. Amongst the points that could lead to a discussion and be mentioned in a statement, should they not be addressed in the final EU-US Privacy Shield adequacy decision, the BTLE identified the independence and powers of the Ombudsperson and the issue related to the remaining possibility to collect data in bulk. In this regard, the WP29 **awaits the CJEU upcoming opinion and decision in cases relating to bulk collection of data.**

REGARDING POSSIBLE ACTIONS **AFTER** ADOPTION OF THE PRIVACY SHIELD ADEQUACY DECISION

Once the UE-US Privacy Shield adequacy decision will have been published, it has been agreed within the FOP that the WP29 will issue **a public statement** specifying, in particular, whether it is satisfied or dissatisfied with the final version.

Besides, in case the published adequacy decision still cannot be considered as satisfactory, the possibility for DPAs to **seize directly their national judge** was envisaged during the ITS subgroup. Nevertheless, the FOP subgroup discussion confirmed that **none** of the attending DPAs **has the power** to directly seize its national judge to refer the finalized EU-US Privacy Shield adequacy decision to its review and obtain that it requests a preliminary ruling from the CJEU.

REGARDING POSSIBLE ENFORCEMENT ACTIONS

If the final adequacy does not provide sufficient safeguards according to WP29's opinion, the ITS subgroup discussed what could be criteria for action from DPAs on companies transferring data to the US (for cases where there is no complaint).

The ITS subgroup started elaborating on **the possible scenarios and criteria for action from DPAs on companies transferring data to the US.** It was suggested to **prioritize** action towards companies which put the most individual at stake and for which there is a suspicion of mass surveillance (e.g. the list of companies allegedly implicated in Snowden's revelations).

On the contrary, criteria based on the type or the volume of data might not be the most relevant (For pharmaceutical data: even if it's massive, it might not be of great interest for intelligence services. On the other hand, Snowden's revelations showed that the aim of intelligence service is to have as much data as they can have. It's not targeted gathering anymore in an era of big data. There is no data that is not of interest anymore).

The work carried out so far confirms that it is rather complex to draft a proper action plan in case of infringement of the EU legal system.

Delegations which took part to the FOP subgroup collectively insisted that the members of the WP29 have to agree on the need to **act in a coordinated way** and, if so, need a clear commitment to act as such. This is a preliminary requirement that should be satisfied before any action plan can exist/be drafted.

**The resulting strategy should be a common and coherent one.**

REGARDING EFFECTS ON OTHER TRANSFER TOOLS

Any conclusion the WP29 draws on the adequacy of the level of protection offered in the U.S. will not only have effect on the Privacy Shield, but also on the other transfer tools.

While the Privacy Shield is still subject to a final decision by the Commission, following prior approval from the Article 31 Committee, the other tools for transfer are already in place.

The consequence of the Opinion may therefore be that data transfers made on the basis of one of the other transferring tools, enforcement actions might be required on a case-by-case basis.

As a result, the **discussions** on the effects on alternative instruments, which already started in the subgroups last year, **will also have to be continued in the light of the outcome of the Privacy Shield adequacy decision.** The ITS subgroup proposed that this work include **updating** the WP29's **previous opinion on adequacy** (WP12) to take into account the CJEU Schrems decision.

It was also suggested that the WP29 **consults/hears data controllers** on the measures they would like to use (encryption, rely on mechanisms like consent…) in order to continue transferring data to the US in case the Privacy Shield is not considered to be satisfactory. This is even more relevant for DPAs that do not have a prior authorization competence and will at least need to start questioning data controllers.

ON POTENTIAL ENFORCEMENT ACTIONS ON TRANSFERS STILL BEING MADE UNDER THE INVALID SAFE HARBOR

It results from the discussions that **four DPAs** (ES, IE, DE, FR) launched procedures against companies supposed to still be using the Safe Harbor as a basis for transfers of personal data to the US. These **ongoing procedures** are mostly confidential. Some others either received no complaint or are not aware of such transfers.

**Action requested from the Plenary**

The plenary is requested to:

- **Discuss the next steps** points identified within the ITS and the BTLE subgroup. In particular, discuss the suggestion that **no other opinion** is adopted on the Privacy Shield nor any public statement whatsoever **until the adequacy decision is finalized** by the Commission. **However, once** the UE-US Privacy Shield adequacy decision will have been **published**, it is suggested that the WP29 issues **a public statement** specifying, in particular, whether it is satisfied or dissatisfied with the final version.

- Take a **commitment to act in a coordinated way.**

- **Confirm the mandate of the ITS subgroup** to continue its discussions on the **enforcement action plan** and on the possible consequences on the legality of the **other transfer tools** for data transfers to the United States in case the adequacy decision on the Privacy Shield cannot be considered as offering essentially equivalent protection.

- **Consult/hear the companies** on the solutions they are willing to set up in order to continue to transfer personal data to the US and, more generally, to third countries which do not offer a level of protection that is essentially equivalent to the level of protection offered by the EU legal framework.

**ITEM C.1.a Borders, Travel and Law Enforcement Subgroup – Privacy Shield – Request form Ombudsperson mechanism**

The BTLE subgroup submits for discussion and adoption a common request form for submitting requests under the Ombudsperson mechanism.

The request form has been discussed in detail in the BTLE subgroup. This info note aims to flag the most controversial parts where the BTLE subgroup seeks approval from the plenary.

The BTLE subgroup wishes to recall that the role of the supervisory authorities is limited to verifying the request. What sounds trivial, raises a number of questions however.

The BTLE subgroup has tried to draft a request form which, on the one hand, complies with the obligations set out in the Privacy Shield, and still, on the other hand, does not discourage individuals in the EU from submitting requests by making the submission and the process of verification too demanding.

Additionally, it is the intention of the BTLE subgroup to manage the expectations of the requestor by spelling out the kind of answer the requestor will receive.

- **Degree of verification**

By way of example: The Privacy Shield annex III on the Ombudsperson provides that the supervisory authorities have the obligation to verify that the "request pertains to data reasonably believed to have been transferred from the EU to the United States pursuant to the Privacy Shield, SCC's, BCR's, or Derogations".

This will often be difficult for the requestor to know and, in many cases, it will be difficult for the supervisory authority to "verify". As explained earlier, the BTLE subgroup suggests that the "verification" is understood in a way which does not discourage requests and which does not overburden the supervisory authority. It should be considered necessary if the requester makes a convincing case that his/her data is likely to have been transferred.

In order to verify that a certain email address actually belongs to the requestor, the verification may mean to send an email to the requestor and ask her or him to confirm it.

The document provided by the requestor in order to show that his/her data is likely to have been transferred would not be submitted to the U.S.

- **No limitation to email address**

At the last plenary meeting, the representative of the ODNI explained that the intelligence agencies, in order to identify the requestor and to run the databases, would need to be provided with an email address as a selector search term.

The BTLE subgroup takes the view that the ODNI view is too narrow. A meaningful search by intelligence agencies must include other forms of communication, which do not require an

email address (e.g. WhatsApp), or alternative forms of data processing (e.g. hotel registries in the U.S.).

- **Legal basis of transfer**

While the ITS subgroup has taken the lead on the question of the legal basis, the solution it suggests for U.S. organisations does not work for the requests under the Ombudsperson mechanism. All such requests will be submitted to the U.S. Department of State.

While some delegations prefer to use consent as the legal basis for transfers to the U.S. Ombudsperson, others have expressed their concern about consent. As a pragmatic solution, the BTLE subgroup suggests not using consent, but considers that the derogations for either "defence of claims" or "public interest" could be used as the legal basis. Clarification of the legal basis is sought from the WP29 plenary and, if this is not possible, consideration should be given as to how best to indicate the legal basis for the transfer.

Various delegations have expressed their discomfort with transferring the personal data included in the request form in the absence of any additional information from the U.S. side on the handling of the data received and, in particular, the assurance that it is only processed in the context of the request.

It is suggested that the U.S. Department of State should be contacted by email in order to seek such additional information and assurances. As similar issues may also arise in relation to transfers to the U.S. authorities on the commercial side, this may also tie in with the proposed meeting between the ITS subgroup and the US authorities in mid-March.

**Request to the plenary:**

- **To adopt the request form**
- **To decide whether to use and publish the request form before the U.S. Department of State has provided additional information and assurances as to the personal data included in the request.**

## C.1.b EU-US Privacy Shield – Working document on the Privacy Shield implementation

### Background

During its last Plenary meeting, the Article 29 Working Party discussed the EU-US Privacy Shield implementation measures and decided to:

- vote in favour of the WP29 as being the "EU Centralized Body".

- create a dedicated group under the ITS subgroup, which will be composed of interested ITS experts with the assistance of interested BTLE experts on national security issues/access of public authorities, to work on the implementation of the Privacy Shield (including the Ombudsperson) with the view of presenting a working document to the next December Plenary.

The work was divided between the ITS (in charge of the commercial complaints part) and the BTLE (in charge of the surveillance complaints part). The BTLE and ITS subgroups respectively held their meeting on 15 November and on 17 November 2016.

Members of each subgroup worked on the different aspects of EU-US Privacy Shield implementing measures for the EU DPAs, with a focus on the key subjects identified by the Plenary, namely: communication, complaints forms and procedures, internal rules and EU-US Privacy Shield annual review preparation.

The subgroup discussed and finalized a working document which is presented in Plenary for adoption, containing several documents which are presented for discussion and possible adoption.

### Presentation of the documents submitted to the WP29 Plenary

### List of questions to US authorities

The ITS and BTLE subgroup also finalized, each for their respective parts, a list of questions for the US authorities on the EU-US Privacy Shield implementation.

As representatives of the US DoC and the US FTC will be present to discuss the Privacy Shield in Plenary, this list of questions have been sent to the US authorities in advance.

However, there will be an opportunity given to the Plenary to finalize this list of questions right before the meeting with US representatives.

The ITS subgroup is also asking to the Plenary for a mandate to invite US authorities' contact points (from US DoC and US FTC) to participate in a subgroup meeting for an exchange of views on EU-US Privacy Shield implementation topics.

### Working document (commercial part) – ITS

A dedicated drafting team (BE, DE Federal, DE Bavaria, DE Hessen, EDPS, FR, IT, UK) worked on a **working document on EU-US Privacy Shield implementation measures**, which is submitted to the Plenary for discussion and possible adoption.

This document contains proposals on the following topics:

- Information document and optional common complaint form for EU citizens
- ITS comments on referral forms submitted by US FTC and DoC
- WP29 information material for EU Businesses proposal
- ITS comments on the EU-US Privacy Shield annual review

The contents have been discussed within the ITS dedicated drafting team and have been submitted to all WP29 delegations for peer review and can be proposed for adoption.

However, the ITS wishes to point out the two following elements, which are requiring further discussion within the subgroup.

- **1st discussion point: which tool for framing transfers of personal data to the US authorities?**

The ITS subgroup would like to emphasize in particular one relevant issue, concerning the legal tool to be used for framing the personal data transfers that will occur between EU DPAs and US authorities (US FTC and US DoC) in the context of handling a complaint.

Under the European Commission's decision of 21 July 2016 considered that US Privacy Shield-certified companies can be considered as offering an adequate level of data protection, but however did not cover the US authorities which will receive personal data from the EU DPAs in the context of a complaint handling.

This issue is crucial for both commercial complaints and surveillance complaints made under the EU-US Privacy Shield.

Possible solutions could be: relying on the express consent of the complainant, relying on a derogation based on public interest, or relying on the development of specific tools for cooperation such as Memorandum of Understanding (between EU DPAs and the US DoC and US FTC).

Each solution raises a number of questions. However, the ECJ ruling C-392/14 (Schrems decision) has made a clear duty for EU DPAs to investigate and handle data protection complaints they received from EU data subjects.

Many delegations are of the opinion that EU national DPAs shouldn't rely solely on the consent of the complainant for transferring the data to US authorities.

Moreover, relying on derogations might not be the best move EU national DPAs, firstly because the use of derogations means there are no safeguards protecting the data once transferred, and secondly, especially as the WP29 is pushing other international bodies or organisations (such as IOSCO or ESMA) to implement data protection safeguards in their MoUs.

One option could be to propose to explore to what extent MoUs with the US authorities could be developed.

It is worth noting, in this regard, that the UK, EI and NL DPAs already have (respectively) MoUs in place with the FTC.

As the answer to this issue impacts the very purpose and functioning efficiency of the EU-US Privacy Shield framework, as well as the content of the information and complaint form proposed to be used by EU DPAs for communication purposes to the EU data subjects, the ITS proposes to discuss thoroughly this question of the legal tool for framing transfers of personal data to US authorities as a priority (in its next meeting, our even earlier on a dedicated conference call), and to adopt the document by written procedure when an agreement on the legal basis for transfers question has been found.

Whichever path is chosen, the WP29 need to be aware that law firms and businesses will most likely notice the choice which will be made concerning the legal tool for framing such transfers to US authorities and use it as a template for their own transfers. DPAs might not be able to withdraw from what we are about to communicate on this issue.

- **2nd discussion point: which internal rules of procedure for the EU informal panel of DPAs?**

In order to deal with the drafting of internal working process of the EU informal panel of DPAs, the ITS subgroup decided to rely on an already well-known and flexible cooperation procedure, instead of trying to adapt the previous internal rules of procedure of the previous EU-US Safe Harbor scheme.

Such internal work process could rely, for example, on the existing mutual recognition procedure for BCRs (with one lead DPA, two co-reviewers DPAs if needed, and mutual recognition procedure after a short peer review process).

Due to time constraints, the ITS' subgroup preferred to focus on immediately deliverable documents rather than on internal work processes for EU DPAs. However, in order to ensure quick implementation of the EU informal panel of DPAs, the Plenary is asked to confirm this proposal (this giving to the ITS subgroup guidance on the lines of its future work), and give a mandate to the ITS subgroup to adopt the internal process of work for the EU informal panel of DPAs by written procedure.

**BTLE documents on the setting up of the EU Centralised Body (national security part)**

In a separate note, the BTLE subgroup presents its suggestions on how to make the EU Centralised Body operational. The suggestions have been discussed in part by the entire subgroup. In part they are made the coordinator after consultation with the UK and the Chair.

Apart from the question of the legal basis (consent/public interest/MoU) and other operational issues, it should be noted that the EU DPAs are not the only authorities to which the data subjects can submit requests under the Ombudsperson mechanism. The Privacy Shield provides that requests can be made either to the DPAs or those national authorities competent for the oversight of the intelligence services. It will thus be necessary for all DPAs to find working arrangements with these other national supervisory authority, which are also competent to receive and forward requests. Since the WP29 decided to be the EU Centralised Body and thus the single point of contact on the EU side, it has been considered that all DPAs approach those other supervisory authorities and suggest to them that any request received by them may be forward to the DPAs. The purpose would solely be to make the handling of the requests for all involved more smoothly.

The BTLE subgroup also presents for discussion and, if possible, adoption a common request form to be used by all data subjects who wish to submit a request via the national supervisory authority and the EU Centralised Body to the U.S. Ombudsperson. The form is written in such a way as to enable the national supervisory authorities to verify the request, as required under the Ombudsperson mechanism.

Additional to the question of the legal basis (consent/public interest/MoU), it is still under discussion which information is required to identify the applicant. Whereas the email address is not required for identification purposes, it may be necessary to provide it to the U.S. so that the U.S. side can search their systems to find out if the email address has been accessed. In this scenario, however, it is still under discussion how the supervisory authority can verify that the email address actually belongs to the applicant.

**Annual review**

The BTLE coordinator prepared a first preparatory note on the EU-US Privacy Shield Annual review, on the basis of which the ITS subgroup added some elements.

In order to best anticipate this exercise, the Plenary is asked to decide already on important issues, such as the number of representative of DPAs which will take part in the annual review.

**Publication**

The working document itself is intended to be preparatory work and is not intended to be published. However, some documents it contains are indeed presented for adoption and for publication on the EU DPAs' websites.

The documents for which publication is intended are:

- information and complaint form to the EU informal panel of DPAs (for EU data subjects),
- information for EU businesses on the commercial aspects on the EU-US Privacy Shield,
- complaint forms to the EU centralised body.

**Actions requested from the Plenary**

The Plenary is asked to discuss the following issues and possibly adopt the corresponding document.

1. **WP29 comments on the referral forms drafted by the U.S. Department of Commerce and the US Federal Trade Commission (ITS)**

   See working document, Annex 1, pages 9-10.

   After the hearing of the US authorities, additional comments on the referral forms from the DoC and the FTC might be taken into account.

| The Plenary is asked to discuss and adopt the WP29's comments on US referral forms. |
|---|

2. **Information and complaint form document for EU Citizens related to the commercial aspects of the Privacy Shield (ITS)**

See working document, Annex 1, pages 3-8.

| |
|---|
| The Plenary is asked to discuss the document, and give a mandate to the ITS subgroup to further discuss the issue of the legal tool for framing personal data transfers to US authorities.<br><br>The Plenary is also asked to give a mandate to the subgroup in order to further discuss the information and common form document for EU data subjects and, if possible, have it adopted by written procedure in order to ensure quick implementation of the EU informal panel of DPAs. |

3. **Information document for EU Businesses related to the commercial aspects of the Privacy Shield (ITS)**

See working document, Annex 3 (pages 15-19).

| |
|---|
| The Plenary is asked to discuss and adopt the information document on the EU-US Privacy Shield for EU Businesses (Annex 3 of the working document). |

4. **Internal Rules of Procedure for the EU informal panel of DPAs (ITS)**

| |
|---|
| The Plenary is asked to confirm that the ITS subgroup should developed internal rules by relying on an already well-known and flexible cooperation procedure, such as the already existing mutual recognition procedure for BCRs (with one lead DPA, two co-reviewers DPAs if needed, and mutual recognition procedure after a short peer review process).<br><br>The Plenary is asked to give a mandate to the ITS subgroup to work along these lines for drafting the internal work process for the EU informal panel of DPAs, and once finalised, to have it adopted by written procedure, in order to ensure quick implementation of the EU informal panel of DPAs. |

5. **Common orm for submitting requests to the Ombudsperson via the EU centralised body (BTLE)**

See request form uploaded

| |
|---|
| The Plenary is asked to discuss and, if possible, adopt the form. |

6. **Note on the setting up of the EU centralized body (BTLE)**

See note on the setting up of the EU Centralised Body

| |
|---|
| The Plenary is asked to discuss the note and approve of each suggestions made. The Plenary is asked to give a mandate to the BTLE subgroup to work along these lines for |

drafting the internal work process for the EU Centralised Body, and once finalised, to have it adopted by written procedure, in order to ensure quick implementation.

**7. Note on the preparation of the first annual review of the EU-US Privacy Shield (BTLE & ITS)**

See working document, Annex 2 (pages 11-14)

The Plenary is asked to discuss the content of the document (Annex 2 of the working document) and provide guidance to the subgroups on the proposals.

[redacted]

**From:** JUST ARTICLE29WP SEC (EC)
**Sent:** 02 March 2017 09:36
**To:**

To:

**Subject:** Urgent Written Procedure - draft letter to the U.S. State Department and its annex - deadline 09/03/2017 16:00

**Attachments:** WP29_letter_US_Department of State_final_adoption.doc; Annex_Responses_ Privacy Shield Ombudsperson Mechanism_final_adoption.docx

**Categories:** DPA

Dear Members of the Article 29 Data Protection Working Party,

By decision of the Working Party, **the draft letter to the U.S. State Department and its annex** is hereby submitted to a vote by written procedure.

In this urgent case, the Chair of the Working Party has exceptionally fixed **a deadline of 7 days**.

May I remind you the content of the relevant provisions of the rules of procedure concerning the adoption of documents by written vote:

*"Article 13:*

*The Working Party may decide unanimously to submit a specific question to a written vote.*

*The Chairperson in urgent cases may submit any matter to a written vote.*

*The draft which is subject to a vote shall be sent by the Secretariat to the members entitled to vote in accordance with article 17. The members entitled to vote shall inform the Secretariat of their vote in writing within a term fixed by the Chairperson and in no case in less than fourteen days.* ***However, in urgent cases the Chair may decide to shorten this deadline to at least 7 days****. Failure to inform the Secretariat in such term shall be considered to be an abstention. The Secretariat shall inform the members of the results of the vote. The result of the vote is recorded in the minutes of the following meeting of the Working Party.*

*The written procedure initiated in accordance with paragraph 2 shall be interrupted if one of the members entitled to vote in accordance with article 17 requests within 5 days of receiving the draft that the draft be discussed during a meeting of the Working Party."*

Please indicate clearly if you are in favour (yes), against (no) or you abstain.

**Responses such as "we have no objection", "we agree" or similar will be treated as abstentions.**

Members who are entitled to vote pursuant of Article 17 of the Internal Rules are requested to inform the Secretariat of their vote in writing (either by fax to +32.2.299.80.94 or by e-mail to the following address:

**JUST-ARTICLE29WP-SEC@ec.europa.eu**

**at the latest by 9 March 2017 at 16.00.**

Best regards,

## The Secretariat of Article 29 Working Party

**********

**European Commission**
DG Justice & Consumers
Unit C.3.- DATA PROTECTION
rue Montoyer, 59
Office 02/37
1049 - Brussels
Belgium
+32 2 298 09 91
JUST-ARTICLE29WP-SEC@ec.europa.eu

http://ec.europa.eu/justice/data-protection/index_en.htm
http://ec.europa.eu/justice/newsroom/data-protection/index_en.htm

To the Ombudsperson:

On behalf of the Article 29 Working Party (WP29), as chair, I would like to thank the State Department and the Department of Commerce for attending to the December 2016 plenary of the WP29. The presentation given by your Department regarding the organisational preparations made in order for the Ombudsperson mechanism under the EU-U.S. Privacy Shield to become operational in the United States was very welcome.

Following that meeting, you asked the WP29 questions related to the implementation of the Ombudsperson mechanism by the EU supervisory authorities, in particular related to the setting up of the EU Centralised Body (EUCB). The answers to these questions are annexed to this letter.

I am pleased to inform you that, at its last plenary meeting, the WP29 decided that the data protection authorities (DPAs) of France, the United Kingdom, Bulgaria, Austria and Germany will act on behalf of the EUCB and bring it into operation. Those DPAs are working to establish what is technologically possible in regards to the contact method between the Ombudsperson and the EUCB. This will be a temporary measure until the European Data Protection Board becomes operational in 2018, and until then a compromise solution may have to be reached. My office will provide further information in due course. We also are looking forward to continuing discussions regarding the portal to exchange information regarding requests to the Ombudsperson. Further information as to how the EUCB DPAs see this working is contained in the annex.

As explained in the December meeting, the WP29 considers that it is obliged to provide those EU individuals wishing to submit a request to the Ombudsperson with all the necessary information on how their personal data included will be handled by the Ombudsperson and, in order to respond to the request, with which agencies that personal data will be shared. In this respect, I would be grateful for additional information regarding how the personal data will be retained and for how long, by the Ombudsperson and by the other agencies involved in the process. It would also be appreciated if you could assure us, on behalf of the U.S. agencies involved in the process, that the personal data included in the requests will only be used for the purpose of processing such requests. It would also be helpful if you could confirm whether there are any laws, rules or other restrictions on the way in which any body or person involved in the Ombudsperson mechanism or the in the process is required to handle a request and the information relating to it, for example, any duty of confidentiality.

As I am sure you are aware, the implications of the recent Executive Order 'Enhancing Public Safety in the Interior of the United States' have also been widely discussed in the privacy community. Specifically, different views are expressed as to whether section 14 of this Executive Order impacts on the written assurances provided by the previous US Administration and annexed to the adequacy decision by the European Commission. I would appreciate if you could share your view with the WP29 as to whether the Executive Order or other decisions by the new U.S. Administration have impact on the Privacy Shield and specifically provide confirmation that the new U.S. Administration continues to honor those assurances.

The first joint annual review, in the autumn of 2017, will be a key moment for the robustness and efficiency of the Privacy Shield mechanism to be further assessed including the effect of any legislative changes made since the adoption of Privacy Shield.

Please be assured that the WP29 looks forward to continuing to work together with the new U.S. administration in order to fulfil the joint responsibilities our institutions have under the new Ombudsperson mechanism.

Sincerely,

Chairwoman of the WP29.

**Privacy Shield Ombudsperson Mechanism**
**Questions for Article 29 Working Party**

## Role of EU Individual Complaint Handling Body

1. Thank you for confirming that the Article 29 Working Párty is the designated "EU Individual Complaint Handling Body." Who will serve as the Ombudsperson's staff primary point(s) of contact and where will the contact(s) be located?

   *The Article 29 Working Party (WP29) has chosen the Data Protection Authorities of A, B, and C (D and E) to serve as the DPAs to make the EU Centralised Body operational in its initial stages. The EU Centralised Body (EUCB) can be contacted through the newly created email address XXX, which will be administered by the Chair of the WP29. WP29 will provide notification of any changes to the DPAs or other supervisory authorities involved in the EUCB.*

2. We understand some member state data protection authorities DPAs intend to serve as the first point of contact with relevant EU individuals who wish to submit a complaint. Will the EU Individual Complaint Handling Body also receive complaints directly from EU individuals?

   *No, it is the understanding of the WP29 from Annex III that requests have to be submitted initially to a national supervisory authority either with oversight for national security services or the processing of personal data by public authorities. The WP29 agrees that it should always be the task of the national supervisory authority to verify the request. The role of the EUCB is, in the view of the WP29, limited to ensuring consistency regarding the process of verification, checking the complaint is complete, serving as the single point of contact with the U.S. side and transmitting the request to the Ombudsperson.*

3. For complaints submitted as an initial matter to a DPA, what is the process for transferring those complaints (and the relevant personal information that accompanies a complaint) to the EU Individual Complaint Handling Body?

   *Requests will be verified by the national supervisory authority and, only once it has been verified and all necessary determinations are made will it be*

*forwarded to the EUCB, which will ensure that the verification etc. is done consistently. The EUCB will transmit all requests to the Ombudsperson.*

4. How will the EU Individual Complaint Handling Body verify that (a) an individual is eligible to submit a complaint under the Privacy Shield Ombudsperson mechanism and (b) the request is "complete" as defined in Section 3.b. of Annex A of the Privacy Shield Framework?

   *The national supervisory authority will check the identity of the requestor. It will also require that the requestor provides any relevant selector search term and as well as confirmation as far as reasonably possible that such search terms belong to the requestor. As to the other requirements not related to the identity, the supervisory authority will assess whether the information provided is sufficient in light of section 3.b of Annex A. The requestor will have to ensure in the request form that all relevant information is correctly provided.*

**Ombudsperson Mechanism Submission Portal**

1. At the December 2016 plenary meeting, we shared our decision to establish a password-protected portal accessible by a small number of individuals acting on behalf of the EU Complaint Handling Body, each with a unique user account, to transmit Ombudsperson Mechanism review requests. How many people do you envisage having responsibility for submitting Privacy Shield Ombudsperson requests to the United States?

   *The WP29 welcomes the confirmation that Department of State has established a platform which will help to make the transmission of information easier. The EU DPAs which make up the EU Centralised Body should have access to this platform. Only a limited number of staff in each DPA will be granted access to the user account.*

2. In our experience, using individual points of contact and their email addresses at the Article 29 working party is not efficient, given that people can be absent due to issues such as illness or vacations, or may change jobs. Do you have a group email address or listserv for us to send confirmations of receipt and other correspondence related to submissions to the portal?

*We will ensure that those DPAs which act on behalf of the EU Centralised Body create a new email address for that purpose / that the Chair will create a new email address for that purpose.*

3. The EU Complaint Handling Body will need to upload copies of the original request, an English translation if the original request is in a language other than English, and any related documents for the Ombudsperson (not to include information provided for verifying the individual requestor's identity or unrelated contact information). We want to ensure that our system is compatible with any information you submit. What formats (.pdf, .docx, etc.) does the EU use for maintaining documents?

   *We understand that the EU Centralised Body will transmit via the platform of the State Department all information needed to show that the request is complete. It is suggested that we are enabled to upload a standardized document, in the form of a .pdf, which includes all relevant information. As agreed in the last plenary meeting, this will not, however, include any information provided by the requestor to prove his or her identity, but simply confirmation that it has been verified by the appropriate supervisory authorities.*

4. Have you received any Ombudsperson-related requests yet? If so, when would you expect to be able to evaluate them and, if they are found sufficient, submit them to us?

   *The WP29 is only aware of one request which, in the current form, has not been found to be within the scope of the Ombudsperson mechanism and has thus been rejected.*