EUROPEAN DATA PROTECTION SUPERVISOR

LEONARDO CERVERA NAVAS
DIRECTOR

Ms [redacted]

by email only:
[redacted]

Brussels, 14 June 2021
LCN/TT/ktl/D(2021)1340 **C 2020-1124**
Please use edps@edps.europa.eu for all correspondence

Subject: **Your Confirmatory Request for access to documents under Regulation (EC) 1049/2001**

Dear Ms [redacted]

On 2 December 2020, you sent an access to documents request to the European Data Protection Supervisor ("EDPS") on the basis of Regulation (EC) 1049/2001, which was registered on the same day.

Your request concerned the following:

> *"a) the mapping exercise that the EDPS has carried out following the Schrems II judgment, including any related report detailing the outcome (the EDPS published a strategy document requiring EU institutions to carry out such exercise . I expect that the EDPS must have done one for itself).*
>
> *b) If the EDPS uses any of the following tools: Microsoft Office365, Microsoft Teams, Zoom, Cisco Webex, Skype, I request any privacy assessment or similar document (including DPIA) done by the EDPS in view of adopting the use of* such *tools. Kindly note that I do not want generic guidelines. Instead I seek specifically any privacy assessment that relates to the internal use by the EDPS of any of the tools I listed.*
>
> *For both categories of documents you can redact any personal data and any information that would imperil the security of your IT systems.".*

By letter of 14 January 2020, we informed you that the EDPS could not provide you with access to the documents related to your request of access to documents linked to EDPS mapping exercise and DPIA as they fall within the exceptions of art. 4(3) of Regulation 1049/2001.

On 22 January 2021, you submitted a confirmatory application, reiterating your request for access to the documents listed above, by arguing that (i) "*the report that yourself confirmed exists must be considered as final; hence it cannot fall under the exception of art. 4(3)",* (ii) EDPS did not provide the status or information if any other document exists at all, (iii) "*the exceptions of art. 4(3) of Regulation 1049/2001 cannot apply*" as EDPS "*did not provide any argument or explanation at all on why disclosure would seriously undermine the decision making process*" and (iv) existence of *"overriding public interest for disclosure".*

By letter of 08 February 2021, we informed you that the EDPS confirmed its position and could not provide you with access to the requested documents, as they are part of ongoing procedure, where the decision is not yet taken by EDPS and thus fall within the exceptions of art. 4(3) of Regulation 1049/2001.

On 12 February 2021, the European Ombudsman ("EO") informed us that following your complaint before this institution, it had opened an inquiry regarding the EDPS's decision to refuse access under Regulation 1049/2001. Following several meetings and exchanges of communications, by letter from 26 April 2021 the EO informed us that considered "*it reasonable for the EDPS to conclude that disclosure of the report on the EDPS mapping exercise is likely to undermine the purpose of the ongoing investigation, as protected by Article 4(2), third indent, of Regulation 1049/2001. I note - and welcome - that the EDPS committed during the meeting with my inquiry team to reconsider partial or, if possible, full disclosure of the document at a later stage."*

With the same letter, the EO proposed *"that the EDPS now reviews its position on the second part of the complainant's public access request, taking into account my above observations, with a view to granting the widest possible public access to the identified documents."*

Having in mind the EDPS's commitment to transparency and following the proposal from the EO, the EDPS has decided to review its Confirmatory Response by re-examining specifically the requested documents in order to assess whether at least partial disclosure is possible. You will find hereafter the EDPS's renewed analysis and response to your confirmatory request dated 22 January 2021.

Pursuant to our renewed analysis of the documents you requested in your initial request of 2 December 2020, the EDPS has concluded the following:

1) The exception of Article 4(2), third indent, of Regulation 1049/2001 (disclosure would undermine the protection of the purpose of inspections, investigations and audits) still applies to the documents falling within the scope of the first part of your request. In particular, disclosure at this point in time of the mapping exercise relating to the implementation of the Schrems II judgment may endanger the completion of the exercise by

hindering cooperation on the part of the supervised European Institutions and bodies subject to it. We note that the CJEU has clarified that the concept of "investigation" is likely to also cover the activity aimed at ascertaining facts in order to assess a given situation1. In that context, the EDPS, using its investigatory powers may gather and analyse information relating to the implementation of data protection requirements by the supervised institutions and bodies.

However, we have identified two documents to which we decided to grant you full access:

1. Letter from EDPS to the heads of all Union institutions, bodies and agencies dated 2 October 2020
2. Letter from EPDS to DG ITEC dated 23 October 2020

Moreover, we would like to inform you that we plan updating the public about the developments of our investigation via our Press Office. Please follow EDPS website for relevant press releases and information.

2) With regards to the second part of your request - "*privacy assessment or similar document (including DPIA) done by the EDPS of the following tools: Microsoft Office365, Microsoft Teams, Zoom, Cisco Webex, Skype"* we have identified to following documents falling within the scope of your request:

	DOC ID	DATE	TYPE	NAME	ACCESS
1	COO.6515.100.2.431394	11/07/2019	WORD	ZOOM Assessment	FULL
2	COO.6515.100.2.396786	23/04/2020	EXCEL	VC tools v.1.2	FULL
3	COO.6515.100.2.404299	07/09/2020	EXCEL	VC tools v.1.3	FULL
4	COO.6515.100.4.396865	27/04/2020	WORD	Note to the file	FULL
5	COO.6515.100.2.405488	16/09/2020	WORD	EDPS INSPECTION TOOLS v.2	NONE
6	COO.6515.100.4.404299	07/09/2020	WORD	EDPS INSPECTION TOOLS	NONE

The EDPS would like to inform you that it has granted you access to four of the documents identified (1-4), with the exception of personal data of the staff members involved in the correspondence, in accordance with Article 4(1)(b) of Regulation 1049/2001.

The documents under part 2 of your request not disclosed by the EDPS (5 and 6) fall within the exceptions of Article 4(2), third indent, of Regulation 1049/2001 as they contain details of the working tools and methods utilized during our inspections. In this regard, the disclosure of the said documents containing information about the EDPS-s internal methodologies could compromise the effective use of the EDPS's means of investigation in the future.

Finally, please note that pursuant to Article 8(1) of the Regulation (EC) 1049/2001, you are entitled to initiate proceedings before the Court of Justice of the European Union against

[1] Judgment of the General Court of 4 October 2018 in case T-128/14, Daimler v Commission.

this Confirmatory Response of the EDPS, under the conditions laid down in, respectively, Article 228 and 263 of the Treaty on the Functioning of the European Union.

Yours sincerely,

[redacted]

Cc: Ms Emily O'REILLY, European Ombudsman
Ms Rosita HICKEY, Director of Inquiries, EO

Annexes: 6 files

Data Protection Notice

According to Articles 15 and 16 of Regulation (EU) 2018/1725 (the Regulation) on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, we are processing your personal data, where proportionate and necessary, for the purpose of answering your request. The legal base for this processing operation is Regulation (EC) 1049/2001 and Article 52(4) of the Regulation (EU) 2018/1725. Subject to applicable rules under EU legislation, the personal data relating to you, as provided in your request as well as personal data that might be collected while processing your request, are used solely for the purpose of replying to your request. EDPS staff members dealing with the request will have access to the case file containing your personal data on a need-to-know basis. All access to case files is logged. Your personal data are not disclosed outside the EDPS. Your personal data will be stored electronically for a maximum of ten years after the closure of the case, or as long as the EDPS is under a legal obligation to do so. You have the right to access your personal data held by the EDPS and to relevant information concerning how we use it. You have the right to rectify your personal data. Under certain conditions, you have the right to ask that we delete your personal data or restrict its use. We will consider your request, take a decision and communicate it to you. For more information, please see Articles 14 to 21, 23 and 24 of the Regulation. Please note that in some cases restrictions under Article 25 of the Regulation may apply. Any request to exercise your rights should be addressed to the EDPS

at edps@edps.europa.eu. You may contact the data protection officer of the EDPS (EDPS-DPO@edps.europa.eu), if you have any remarks or complaints regarding the way we process your personal data. You have the right to lodge a complaint with the EDPS, as supervisory authority. Any such request should be addressed to the EDPS at edps@edps.europa.eu. You can reach the EDPS in the following ways: E-mail: edps@edps.europa.eu; EDPS postal address: European Data Protection Supervisor, Rue Wiertz 60, B-1047 Brussels, Belgium. For more information, please refer to the extended version of the data protection notice available on the EDPS website: https://edps.europa.eu/data-protection/our-work/publications/other-documents/requests-access-documents_en.

EUROPEAN DATA PROTECTION SUPERVISOR

WOJCIECH RAFAŁ WIEWIÓROWSKI
SUPERVISOR

To the heads of all Union institutions,
bodies and agencies

Brussels, 2nd October 2020

[redacted] D(2020) 2169 **C 2020-0766**
Please use edps@edps.europa.eu
for all correspondence

Subject: Order of the EDPS pursuant to Article 58(1)(a) of Regulation (EU) 2018/1725 to provide information

Dear Sir or Madam,

On 16 July, the Court of Justice of the EU issued the Judgment in case **C-311/18**, known as 'Schrems II' (the 'Judgment'), concerning Commission Decision 2010/87/EC on Standard Contractual Clauses ('SCCs') for transfers to third countries in general and the level of protection ensured in the United States in particular (Privacy Shield[1]). As this Judgment has serious implications on personal data transfers carried out by Union institutions, bodies, offices and agencies ('EUIs'), I address this letter to you in order to inform you about the information I expect your institution to provide.

I. Background information

The Court in its Judgment notably ruled the following:

- The Privacy Shield is invalidated in particular on the basis of (i) the lack of proportionality caused by mass surveillance programmes based on Section 702 of the FISA[2] and E.O.[3] 12333 read in conjunction with PPD-28 and (ii) the lack of effective remedies in the US essentially equivalent to those required by Article 47 of the Charter.
- The validity of the 2010 Standard Contractual Clauses ('SCCs') for transfers is confirmed (Commission Decision 2010/87/EC). However, that validity, depends on whether the SCCs include effective mechanisms to ensure compliance in practice with the level of protection essentially equivalent to that guaranteed within the EU by the General Data Protection Regulation ('GDPR')[4] and the transfers of personal data pursuant to such clauses are suspended or prohibited in the event of the breach of such clauses or in case it is impossible to honour them.

1 Commission Decision 2016/1250 on the adequacy of the protection provided by the EU-U.S. Privacy Shield.
2 Foreign Intelligence Surveillance Act
3 Executive Order.
4 This is to be understood as a reference to the similar provisions of Regulation (EU) 2018/1725 for the EUIs.

- The SCCs for transfers may then require, depending on the prevailing position in a particular third country, the adoption of 'supplementary measures' by the controller in order to ensure compliance with the level of protection guaranteed within the EU.
- Commission Decision 2010/87/EC imposes an obligation on the data exporter (controller) and the recipient of the data (the 'data importer') to verify, prior to any transfer, and taking into account the circumstances of the transfer, whether that level of protection is respected in the third country concerned. The Commission Decision 2010/87/EC further requires the data importer to inform the data exporter of any inability to comply with the standard data protection clauses, and where necessary with any supplementary measures to those offered by those clauses, the data exporter then being, in turn, obliged to suspend the transfer of data and/or to terminate the contract with the data importer. However, if the controller intends to keep transferring data despite this conclusion, it must notify their competent supervisory authority.
- The competent supervisory authority is required to suspend or prohibit a transfer of data to a third country pursuant to standard data protection clauses adopted by the Commission, if, in the view of that supervisory authority and in the light of all the circumstances of that transfer, those clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer.

The Judgement has far-reaching consequences as the threshold set by the Court is meant to apply to all appropriate safeguards provided by controllers or processors under Article 46 GDPR[5] in order to transfer data from the European Economic Area (EEA) to any third country.

The European Data Protection Supervisor (EDPS) is the independent supervisory authority established by Article 56 of Regulation (EU) 2018/1725 ('the Regulation')[6]. It is the duty of the EDPS under Article 57(1)(a) and (f) of the Regulation to monitor and ensure the application of the Regulation with regard to the processing of personal data by any EUI, including through the use of its corrective powers pursuant to Article 58(2) of the Regulation.

Therefore, pursuant to Article 58(1)a of the Regulation, I ask you to provide information concerning on-going processing operations and contracts involving transfers to third countries (II)while paying special attention to new processing operations and contracts that would involve such transfers (III).

II. Information required from your EUI concerning on-going processing operations and on-going contracts involving transfers to third countries

In this respect, I ask you to provide the following information:

1. **Mapping exercise** (to be concluded by 31 October 2020)

In order to enable the EDPS to fulfil its tasks under Article 57 of the Regulation and for the EUIs to comply with the present order and the Regulation, it is necessary that EUIs carry out a mapping of data flows.

---

[5] This is to be understood as a reference to Article 48 of Regulation (EU) 2018/1725 for the EUIs.

[6] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC; OJ L 295, 21.11.2018, p. 39.

In this respect, I would like to ask you to **launch immediately**[7] **a mapping exercise** with the aim to map data transfers (including onward transfers) for on-going contracts and procurement procedures and other types of cooperation in the context of which personal data is transferred. The mapping exercise is to list in particular:

- each processing activity for which data is transferred to / accessed from a third country (including purposes and means of processing);
- destinations of data transfers (including those of all processors and sub-processors);
- type of recipient (data importer);
- transfer tool used (of the ones provided in Chapter V of the Regulation);
- types of personal data transferred;
- categories of data subjects affected;
- any onward transfers (including to which countries and which recipients, transfer tool used, types of personal data and categories of data subjects affected).

Your records of processing activities (Article 31 of the Regulation) are a good starting point for this task. You should also check the contracts you have with processors and with other controllers, as well as other arrangements you might have in the context of which personal data is transferred. In line with Article 31(2) of the Regulation, each processor shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing inter alia information on international transfers of personal data. At the end of this task, you should be able to locate where exactly the personal data you exported may be. Note that remote access (e.g. in support situations) is also considered a transfer.

2. **Report to the EDPS any identified risks and gaps based on the mapping exercise** (at the latest by 15 November 2020). The following cases should be reported to the EDPS:
    1) Transfers which are not based on any transfer tool (e.g.: onward transfers between the EUI's processor and a sub-processor that are not framed by any standard or *ad hoc* contractual clauses or another arrangement);
    2) Transfers that are based on a derogation under Article 50 of the Regulation;
    3) 'High-risk transfers' to the US in light of the Judgment. Those "high-risk transfers" concern any transfer to entities clearly subject to Section 702 FISA or E.O. 12333[8] ***and*** involving:
        - large scale processing operations[9]; *or*
        - complex processing operations or sets of operations[10]; *or*
        - processing of sensitive data or data of a highly personal nature[11].

---

[7] We strongly recommend launching the exercise without delay as the input of the data importers (processors/sub-processors) is likely to be required in order to complete the exercise.

[8] Section 702 FISA applies to all "electronic communication service provider" (see the definition under 50 USC § 1881(b)(4)), while EO 12 333 organises electronic surveillance, which is defined as the "acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a non electronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter" (3.4; b)).

[9] See EDPS reply to informal consultation on the application of Article 39(3)(b) of Regulation (EU) 2018/1725. See also Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248 rev.01, adopted by the Article 29 Working Party and endorsed by the EDPB.

[10] For example processing operations involving large datasets of complex data structure, linking different databases, big data analytics, the use of novel technologies or complex techniques (like those in profiling and automated-decision making processes), or involving many different or unknown actors.

[11] See Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248 rev.01, adopted by the Article 29 Working Party and endorsed by the EDPB, pages 9-10: "*4. Sensitive data or data of a highly personal nature: this includes special categories of personal data as defined in Article 9 (for example information about*

The report should mention the risks under case 3) and explain all mitigating measures taken to address those risks. These reports should provide sufficient information for the EDPS to understand the transfers mentioned under the cases 1) to 3) above, as well as the risks and what measures, if any, the EUIs had put in place. In particular, all the information requested for the mapping exercise under point 1 in relation to the particular processing activity and transfer concerned should be included.

Your EUI should require the help of processors and/or other data importers to identify transfers (including onward ones) and destinations for personal data processed on behalf of the EUI. While your DPO is to be closely associated in dissemination of information to controllers and later in gathering and synthesising information in the report to the EDPS, the primary responsibility lies with the controllers of the data processing within your EUI.

3. **Further steps**

The abovementioned mapping exercise will help EUIs to carry out, **in a second phase,** case-by-case "transfer impact assessments" ('TIA') with the aim to identify whether an essentially equivalent level of protection as provided in the EU/EEA is afforded in the third country of destination. The factual description of the circumstances of each transfer should be based on the mapping exercise done by data exporter and should include additional information provided by data importer. Identification and implementation of 'supplementary measures' or 'additional safeguards' may be necessary in order to ensure such equivalence in the level of protection[12]. The circumstances of the transfer will also influence the identification of any appropriate supplementary measures.

Concluding this second phase, EUIs should reach a decision as to whether it is possible to continue the transfers identified in the mapping exercise (with appropriate safeguards and supplementary measures or based on a derogation).

With the aim to facilitate TIAs, the EDPS will provide EUIs in due time with guidance on the elements that they should take into account when conducting such assessments, as well as with guidance on supplementary measures. Possible further guidance issued in the meantime by the European Data Protection Board will be taken into account[13].

Let me recall that in line with Article 46 of the Regulation, any transfer of personal data to a third country or international organisation shall take place only if, subject to the other provisions of the Regulation, the conditions laid down in Chapter V are complied with, including for

---

individuals' political opinions), as well as personal data relating to criminal convictions or offences as defined in Article 10. An example would be a general hospital keeping patients' medical records or a private investigator keeping offenders' details. Beyond these provisions of the GDPR, some categories of data can be considered as increasing the possible risk to the rights and freedoms of individuals. These personal data are considered as sensitive (as this term is commonly understood) because they are linked to household and private activities (such as electronic communications whose confidentiality should be protected), or because they impact the exercise of a fundamental right (such as location data whose collection questions the freedom of movement) or because their violation clearly involves serious impacts in the data subject's daily life (such as financial data that might be used for payment fraud). In this regard, whether the data has already been made publicly available by the data subject or by third parties may be relevant. The fact that personal data is publicly available may be considered as a factor in the assessment if the data was expected to be further used for certain purposes. This criterion may also include data such as personal documents, emails, diaries, notes from e-readers equipped with note-taking features, and very personal information contained in life-logging applications."

[12] See paragraph 133 of the Judgment and recital 66 of the Regulation.

[13] Please note that a first set of FAQs was adopted by the EDPB on 23 July 2020. See also the statements of the EDPS and the EDPB following the Schrems II judgement.

onward transfers. I wish furthermore to underline the limited use of derogations pursuant to Article 50 of the Regulation[14]. The EDPS in its supervisory activities will put special attention to control if derogations are used properly.

III. New processing operations and new contracts that will entail transfers of personal data

The EDPS' own-initiative investigation into the use of Microsoft products and services by EUIs and our recommendations to the EUIs in that regard confirm the importance of ensuring a level of protection essentially equivalent to that guaranteed within the EU by EU data protection laws, read in light of the Charter. The EDPS already flagged in this context a number of linked issues concerning sub-processors, data location, international transfers and the risk of unlawful disclosure of data – issues that the EUIs were unable to control and ensure proper safeguards to protect data that left the EU/EEA. The issues we raised in our investigation report are consistent with concerns of the Court in its Judgment, which we are assessing in relation to any processors of the EUIs.

In light of the above and following the Judgment, , the EDPS is convinced that EUIs need a strong precautionary approach as regards the use of any service provider and any new processing operations. For this reason, the EDPS strongly encourages that EUIs ensure that any new processing operations or new contracts with any service providers, involve no transfers of personal data to the U.S. In this regard, please note that any enforcement actions by the EDPS to ensure compliance with the Regulation will also cover future activities of EUIs, not only those that took place before the receipt of this letter.

As a community of EUIs, we believe it is our common duty to protect the rights of individuals and safeguard their personal data, including when transferred to third countries, stemming from the Charter of Fundamental Rights, the Regulation and the jurisprudence of the Court of Justice of the European Union. Your cooperation in applying the Court's Judgment is therefore of utmost importance.

Yours sincerely,

[**E-signed**]

Wojciech Rafał WIEWIÓROWSKI

cc: Data Protection Officer of your institution

[14] In this respect, see also the EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679.

EUROPEAN DATA PROTECTION SUPERVISOR

LEONARDO CERVERA NAVAS
DIRECTOR

Mr Walter PETRUCCI
Director-General
Directorate-General for Innovation
and Technological Support
Rue Belliard 89
B-1040 Bruxelles

Brussels, 23 October 2020
[redacted] D(2020) 2399 **C 2020-0940**

Subject: **Mapping of transfers of personal data to third countries (EDPS order of 2 October 2020. EDPS case 2020-0766) [EDPS DPO case 2020-0940]**

Dear Mr Petrucci,

Following the Court of Justice of the EU judgment in case C-311/18 (known as 'Schrems II'), on 2 October 2020, the European Data Protection Supervisor - EDPS - (as the supervisory authority) contacted all heads of administration of European Union institutions, bodies and agencies (EUIs) requesting information on transfers to third countries (outside EEA) of personal data processed by their respective EUI (appendix 1).

Myself, as head of administration of the EDPS, also received the same request from the Supervisor because we are also concerned about this judgement in our role as data controllers. As you know, the EDPS, for its own purposes and on behalf of the EDPB, signed a Service Level Agreement (SLA) on the use of IT support services with the EP (DG ITEC), a service that it is essential for our business continuity and that we appreciate so much. The SLA defines the EP as a processor for any processing operations involving the EDPS and the EDPB as sole or joint controllers.

In order to be able to address the request of the Supervisor, as I am sure that your own services are doing, we are updating our mapping of international data transfers. In this context, I would be grateful if your services could provide us information regarding personal data processing (taking place within the framework of the SLA) that might entitle transfers of personal data to third countries. If any such transfers take place, we would appreciate if you could provide us with the following information (requested in the above-mentioned letter of 2 October):

- each processing activity for which data is transferred to / accessed from a third country (including purposes and means of processing);
- countries of destinations of data transfers (including those of EP's processors and sub-processors);
- type of recipient (data importers);
- transfer tool used (of the ones provided in Chapter V of the Regulation 2018/1725);
- types of personal data transferred;
- categories of data subjects affected;
- any onward transfers (including to which countries and which recipients, transfer tool used, types of personal data and categories of data subjects affected).

I hope that you can understand that we are unable to get this information by ourselves and this is the only reason why we are requesting your kind cooperation. We would be very grateful if you could provide us with this information by **4 November**. I am aware that the deadline is very tight. However, given that the request made on 2 October concerns also the EP, I believe that it is likely that this information will be already available as a result of the analysis conducted by the EP in order to reply to said request.

I am looking forward to your reply and remain available for any clarifications that you may need. Thank you in advance for your cooperation.

Best regards,

[redacted]

Appendix 1: Order of the EDPS pursuant to Article 58(1)(a) of Regulation (EU) 2018/1725 to provide information

Cc.: [redacted]

Name of service	Web site	Wikipedia	Provider	Provider location	Hosting	Open source	Price	User limit
Zoom	Zoom	wiki_zoom	Zoom Video Communication Inc.	San Jose, CA, U.S.	self-hosting possible in Business plan	no	4 plans	
GoToMeeting	GoToMeeting	wiki_GoToMeeting	LogMeIn	Boston, MA, U.S.	both in cloud and on-premise hosting available	no	3 plans	
GoToWebinar	GoToWebinar	N/A	LogMeIn	Boston, MA, U.S.	only web-based	no	3 plans	
CyberLink U Meeting	CyberLink U Meeting	wiki_Cyberlink	CyberLink Corp.	New Taipei City, Taiwan	no self-hosting	no	4 plans	
BlueJeans	BlueJeans	wiki_BlueJEans	BlueJeans Network	San Jose, CA, U.S.	Premise-to-Cloud Integration in Enterprise plan	yes GitHub	3 plans	
Google Hangouts Meet	Google Hangouts Meet	wiki_GHangouts	Google LLC	Mountain View, CA, U.S.	no self-hosting	no	free	100

Cisco WebEx	Cisco WebEx	wiki_WebEx	Cisco Webex, BT cloud		no self-hosting	no	4 plans	300
Cisco Jabber	Cisco Jabber	N/A	Cisco	U.S.	self-hosting possible	no		2
Cisco Webmeeting	Cisco Webmeeting	N/A	Cisco		self-hosting possible	no		10 in personal room, 25 in booked room
Skype for Business	Skype for Business	wiki_SkypeforB	Microsoft	Redmonds, WA, U.S.	no self-hosting	no	free	250
Microsoft Teams	MS Teams	wiki_MSTeams	Microsoft	Redmonds, WA, U.S.	no self-hosting, cloud only	no	free w/office365 subscription	300
Jitsi	Jitsi	wiki_Jitsi	8x8 Inc.	N/A	self-hosting possible	yes GitHub	free	75
Bigbluebutton	Bigbluebutton	wiki_Bigbluebutton	Bigbluebutton Inc.	Ottawa, Canada	self-hosting possible	yes Github	free	100
Apache OpenMeetings	Apache OpenMeetings	Wiki_AOM	ASF (Apache Software Foundation)	U.S.	self-hosting possible	has OS components	free	N/A
Apple FaceTime	Facetime	wiki_FT	Apple Inc.	Cupertino, CA, U.S.	no self-hosting	no	free	32
Forum Vision	hopin.to		Forum Europe	UK	no self-hosting	no	size-dependent	
Pexip	pexip.com		Pexip Europe	Norway	self-hosting possible	no		

Tixeo	tixeo.com		Tixeo	France	self-hosting possible	no		
Wire Enterprise	wire.com		Wire	Switzerland	self-hosting possible	no		4
Whereby	whereby.com		Whereby	Norway	no self-hosting	no	3 plans	

Web client	Desktop client	Mobile client	Telephone calls	Screen sharing	Moderation[1]	Hand raising	Recording	Room splitting	Link	Complete	Transfers outside of EU
(yes)	yes	yes	yes, add-on	yes	yes	yes	yes	yes, 50 max	Zoom_PP	yes	yes, mainly U.S.
yes	yes	yes	yes	yes	yes	no	yes	no	GoToMeeting_PP	Common LogMeIn PP, referring to the use of websites not of the product.	yes, U.S. and global
yes	yes	yes	yes	yes	yes	yes	yes	no	GoToWebinar_PP	Common LogMeIn PP, referring to the use of websites not of the product.	yes, U.S. and global
yes (Chrome)	yes	yes	no	yes	yes	no	yes	no	U Meeting_PP	no, DPO contact missing	yes, global
yes	yes	yes	yes	yes	yes	yes	yes	yes	BlueJeans_PP	no, Art. 6 GDPR legal bases missing !	yes, mainly U.S.
yes	yes	yes	yes	yes	yes	yes, 'nod' extension	yes	(yes)	Google_PP	yes	yes

yes	yes	yes	yes	yes	yes	yes	yes	no	Cisco_PP	yes, except naming a DPO	yes, 12 data centres worldwide; costumer-generated data stored on the closest server, for us this is Amsterdam, NL. WeBex Analytics data is stored in CA/TEX, U.S, billing data in TEX/NC U.S.
no	yes	yes	no	yes	no	no	yes	no	Cisco_PP		
yes	yes(via Jabber)	yes (via Jabber)	yes	yes			yes	no	Cisco_PP		
yes	yes	yes	yes	yes	no	no	yes	no	Skype for B_PP	yes, except naming a DPO	yes
yes	yes	yes	yes	yes	only channel moderation	yes	yes	no	MS Teams_PP	yes, except naming a DPO	yes, with additional information on the location of data at rest
yes (Chrome)	yes	yes	yes	yes	yes	no	yes	no	Jitsi_PP	yes, together with 8x8 Company Privacy Notice	yes
yes (Chrome, Ff)	yes	yes	yes (VoiP needed)	yes	yes	yes	yes	yes	BigBlueButton_PP	yes (listing only consent as legal basis, strange given the purposes include legal process, "emergency to protect the personal safety of any person")	no indication in PP
	yes	no	yes	yes	yes		yes	yes			
no	yes	yes	yes	yes	no	no	yes	no	FT_PP	yes (except no DPO, only a contact sheet for regions/countries)	yes, personal information of EU/EEA users is controlled by Apple Distribution International Limited in Ireland, and processed on its behalf by Apple Inc
yes (Chrome, Ff)				yes			yes	yes			yes, U.S. and global
				yes							yes, U.S. and global

no	yes	yes		yes							no
yes	yes	yes									yes, Switzerland
yes											

Purposes[4]	PD shared with non-processors	Data Processing Addendum	Link	Complete	Compliant banner	3rd party trackers		End-to-end encryption	User premissions
data centers performance monitoring; aggregated data analytics; respond to support requests; product development; personalised marketing	legal advisors for legal reasons; third party service providers such as public cloud storage vendors, carriers, payment processor	not available	Zoom CP	specific cookies are not listed				no	
research and analysis; data analysis, incl. automated systems and ML for service improvement; personalised marketing communication;	third party service providers; business partners; affiliated companies within the corporate structure; as needed for legal purposes	LogMeIn DPA	integrated in privacy policy, section 3	specific cookies are not listed				no, session data protected by 128-bit AES encryption	
research and analysis; data analysis, incl. automated systems and ML for service improvement; personalised marketing communication;	third party service providers; business partners; affiliated companies within the corporate structure; as needed for legal purposes	LogMeIn DPA	integrated in privacy policy, section 3	specific cookies are not listed				no, session data protected by 128-bit AES encryption	
advertising and direct marketing; provide support and assistance, costumer feedback, further marketing research and data analysis; to meet conract obligations (no details which)	business partners; service vendors; authorized third-party agents or contractors in order to provide Service	not available	integrated in privacy policy, section 3	specific cookies are not listed				only in Enterprise plan	
no explicit list available; advertisment and marketing; product development; to answer to customer requests	business partners, costumers, suppliers, service providers, vendors; auditors, legal advisors, other professional advisors; credit reference agencies	not available	BlueJeans CP	specific cookies are not listed				supports standards-based encryption (AES-128)	
service development; provide personalized services, content and ads; measure performance; improve safety and reliability of service	no data sharing with external companies except: with consent; with domain administrators and reseller who manage accounts; for external processing to affiliates; for legal reasons	not available	not available					yes	

direct marketing; system diagnostics and product developpment; research and analysis of aggregated data	Cisco business partners and vendors, competent DPA or other authority, law enforcement officials and government authorities	not available	not available					yes	
direct marketing; system diagnostics and product developpment; research and analysis of aggregated data	business partners, third parties for legal purposes if needed	Microsoft DPA	Microsoft Cookies	specific cookies are not listed				yes	
diagnostics, service development, direct marketing	business partners, third parties for legal purposes if needed	Microsoft DPA	Microsoft cookies	specific cookies are not listed				yes	
product development	affiliates, a limited number of third-party business partners, service providers, vendors, suppliers and other contractors for the purpose of assisting in providing, managing, deploying, enhancing, or improving services.	not available	not available					yes	
service development; personalized service provision; direct marketing; phone numbers for secondary fraud protection detection	affiliates; third party service providers; disclosure for legal requests or process;	not available	not available	not available				yes (depends on configuration)	
internal purposes, e.g. auditing; direct marketing; product development; research and analysis with anonymised/aggregated data	affiliated service providers; for legal purposes to public and governmental authorities within or outside the country of residence	not available	Apple Use of Cookies	specific cookies are not listed				yes (incl. videostreams)	

								yes (incl. videostreams)	
								yes (incl. videostreams)	

Desktop update frequency[2]	Mobile update frequency[2]	Potential Information Security Risks5	Recent security incidents[3]
4 times over the last 3 months,	4 times during the last 3 months,	to be considered. High probability due to recent security vulnerabilities	Zoombombing
approx 4 updates/month	approx 4 updates/month	to be considered.	
not available	not available	to be considered	
not available	not available	to be considered	
once in every few months, latest March 2020		to be considered	
no separate Hangouts meet product update list available		to be considered	

last updated Jan 31 2020		SLA with EP applies	
		SLA with EP applies	
		SLA with EP applies	
4 times over the last year		To be considered. European Commission assessment applies	
2-3 times/month	once in every few months	To be considered. European Commission assessment applies	
no history of updates available, latest update April 2020		To be considered	
3 times over the last month, now BBB 2.2.5.		To be considered	
		To be considered	
3 system updates over the last year	2 system updates over the last year	To be considered	

Name of service	Web site	Wikipedia	Provider	Provider location	Hosting	Open source	Price	User limit
Zoom	Zoom	wiki_zoom	Zoom Video Communication Inc.	San Jose, CA, U.S.	self-hosting possible in Business plan	no	4 plans	
GoToMeeting	GoToMeeting	wiki_GoToMeeting	LogMeIn	Boston, MA, U.S.	both in cloud and on-premise hosting available	no	3 plans	
GoToWebinar	GoToWebinar	N/A	LogMeIn	Boston, MA, U.S.	only web-based	no	3 plans	
CyberLink U Meeting	CyberLink U Meeting	wiki_Cyberlink	CyberLink Corp.	New Taipei City, Taiwan	no self-hosting	no	4 plans	
BlueJeans	BlueJeans	wiki_BlueJEans	BlueJeans Network	San Jose, CA, U.S.	Premise-to-Cloud Integration in Enterprise plan	yes GitHub	3 plans	
Google Hangouts Meet	Google Hangouts Meet	wiki_GHangouts	Google LLC	Mountain View, CA, U.S.	no self-hosting	no	free	100

Cisco WebEx	Cisco WebEx	wiki_WebEx	Cisco Webex, BT cloud (for the EP setup), Cisco	The Netherlands, but the parent company is US based	no self-hosting	no	4 plans	300
Cisco Jabber	Cisco Jabber	N/A	Cisco	U.S.	self-hosting possible	no		2
Cisco Webmeeting	Cisco Webmeeting	N/A	Cisco	The Netherlands, but the parent company is US based	self-hosting possible	no		10 in personal room, 25 in booked room
Skype for Business	Skype for Business	wiki_SkypeforB	Microsoft	Redmonds, WA, U.S.	no self-hosting	no	free	250
Microsoft Teams	MS Teams	wiki_MSTeams	Microsoft	Redmonds, WA, U.S.	no self-hosting, cloud only	no	free w/office365 subscription	300
Jitsi	Jitsi	wiki_Jitsi	8x8 Inc.	Campbell, CA , U.S.	self-hosting possible	yes GitHub	free	75
Bigbluebutton	Bigbluebutton	wiki_Bigbluebutton	Bigbluebutton Inc.	Ottawa, Canada	Only self-hosting possible	yes Github	free	100
Apache OpenMeetings	Apache OpenMeetings	Wiki_AOM	ASF (Apache Software Foundation)	U.S.	self-hosting possible	has OS components	free	N/A
Apple FaceTime	Facetime	wiki_FT	Apple Inc.	Cupertino, CA, U.S.	no self-hosting	no	free	32

Forum Vision	hopin.to		Forum Europe	UK	no self-hosting	no	size-dependent	
Pexip	pexip.com		Pexip Europe	Norway	Only self-hosting possible	no		
Tixeo	tixeo.com		Tixeo	France	self-hosting possible	no		
Wire Enterprise	wire.com		Wire	Switzerland	self-hosting possible	no		4
Whereby	whereby.com		Whereby	Norway	no self-hosting	no	3 plans	50

Web client	Desktop client	Mobile client	Telephone calls	Screen sharing	Moderation[1]	Hand raising	Recording	Room splitting	Link	Complete	Transfers outside of EU
(yes)	yes	yes	yes, add-on	yes	yes	yes	yes	yes, 50 max	Zoom_PP	yes	yes, mainly U.S.
yes	yes	yes	yes	yes	yes	no	yes	no	GoToMeeting_PP	Common LogMeIn PP, referring to the use of websites not of the product.	yes, U.S. and global
yes	yes	yes	yes	yes	yes	yes	yes	no	GoToWebinar_PP	Common LogMeIn PP, referring to the use of websites not of the product.	yes, U.S. and global
yes (Chrome)	yes	yes	no	yes	yes	no	yes	no	U Meeting_PP	no, DPO contact missing	yes, global
yes	yes	yes	yes	yes	yes	yes	yes	yes	BlueJeans_PP	no, Art. 6 GDPR legal bases missing !	yes, mainly U.S.
yes	yes	yes	yes	yes	yes	yes, 'nod' extension	yes	(yes)	Google_PP	yes	yes

yes	yes	yes	yes	yes	yes	yes	yes	no	Cisco PP	yes, except naming a DPO	yes, 12 data centres worldwide; costumer-generated data stored on the closest server, for us this is Amsterdam, NL. WeBex Analytics data is stored in CA/TEX, U.S, billing data in TEX/NC U.S.
no	yes	yes	no	yes	no	no	yes	no	Cisco PP		
yes	yes(via Jabber)	yes (via Jabber)	yes	yes			yes	no	Cisco PP		
yes	yes	yes	yes	yes	no	no	yes	no	Skype for B PP	yes, except naming a DPO	yes
yes	yes	yes	yes	yes	only channel moderation	yes	yes	no	MS Teams PP	yes, except naming a DPO	yes, with additional information on the location of data at rest
yes (Chrome)	yes	yes	yes	yes	yes	no	yes	no	Jitsi PP	yes, together with 8x8 Company Privacy Notice	yes
yes (Chrome, Ff)	yes	yes	yes (VoiP needed)	yes	yes	yes	yes	yes	BigBlueButton PP	yes (listing only consent as legal basis, strange given the purposes include legal process, "emergency to protect the personal safety of any person")	no indication in PP
	yes	no	yes	yes	yes		yes	yes			
no	yes	yes	yes	yes	no	no	yes	no	FT PP	yes (except no DPO, only a contact sheet for regions/countries)	yes, personal information of EU/EEA users is controlled by Apple Distribution International Limited in Ireland, and processed on its behalf by Apple Inc

yes (Chrome, Ff)				yes			yes	yes			yes, U.S. and global ("By registering for and using Pexip services, you are accepting to the transfer of data to any country in which Pexip and its affiliates maintain facilities") https://support.pexip.com/hc/en-us/articles/208885088-List-of-Pexip-Service-PoPs
				yes							yes, U.S. and global
no	yes	yes		yes							no
yes	yes	yes									yes, Switzerland
yes											

Purposes[4]	PD shared with non-processors	Data Processing Addendum	Link	Complete	Compliant banner	3rd party trackers		End-to-end encryption	User premissions
data centers performance monitoring; aggregated data analytics; respond to support requests; product development; personalised marketing	legal advisors for legal reasons; third party service providers such as public cloud storage vendors, carriers, payment processor	not available	Zoom CP	specific cookies are not listed				no	
research and analysis; data analysis, incl. automated systems and ML for service improvement; personalised marketing communication;	third party service providers; business partners; affiliated companies within the corporate structure; as needed for legal purposes	LogMeIn DPA	integrated in privacy policy, section 3	specific cookies are not listed				no, session data protected by 128-bit AES encryption	
research and analysis; data analysis, incl. automated systems and ML for service improvement; personalised marketing communication;	third party service providers; business partners; affiliated companies within the corporate structure; as needed for legal purposes	LogMeIn DPA	integrated in privacy policy, section 3	specific cookies are not listed				no, session data protected by 128-bit AES encryption	
advertising and direct marketing; provide support and assistance, costumer feedback, further marketing research and data analysis; to meet conract obligations (no details which)	business partners; service vendors; authorized third-party agents or contractors in order to provide Service	not available	integrated in privacy policy, section 3	specific cookies are not listed				only in Enterprise plan	
no explicit list available; advertisment and marketing; product development; to answer to customer requests	business partners, costumers, suppliers, service providers, vendors; auditors, legal advisors, other professional advisors; credit reference agencies	not available	BlueJeans CP	specific cookies are not listed				supports standards-based encryption (AES-128)	
service development; provide personalized services, content and ads; measure performance; improve safety and reliability of service	no data sharing with external companies except: with consent; with domain administrators and reseller who manage accounts; for external processing to affiliates; for legal reasons	not available	not available					yes	

direct marketing; system diagnostics and product developpment; research and analysis of aggregated data	Cisco business partners and vendors, competent DPA or other authority, law enforcement officials and government authorities	not available	not available					yes (see https://www.cisco.com/c/dam/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.pdf)	
								yes (see https://www.cisco.com/c/dam/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.pdf)	
direct marketing; system diagnostics and product developpment; research and analysis of aggregated data	business partners, third parties for legal purposes if needed	Microsoft DPA	Microsoft Cookies	specific cookies are not listed				yes	
diagnostics, service development, direct marketing	business partners, third parties for legal purposes if needed	Microsoft DPA	Microsoft cookies	specific cookies are not listed				yes	
product development	affiliates, a limited number of third-party business partners, service providers, vendors, suppliers and other contractors for the purpose of assisting in providing, managing, deploying, enhancing, or improving services.	not available	not available					yes	
service development; personalized service provision; direct marketing; phone numbers for secondary fraud protection detection	affiliates; third party service providers; disclosure for legal requests or process;	not available	not available	not available				yes (depends on configuration)	
internal purposes, e.g. auditing; direct marketing; product development; research and analysis with anonymised/aggregated data	affiliated service providers; for legal purposes to public and governmental authorities within or outside the country of residence	not available	Apple Use of Cookies	specific cookies are not listed				yes (incl. videostreams)	

								Probably no. See section 8.1 of the privacy policy "Please be aware that internet transmissions are never completely private or secure and that any message or information you send on or using Hopin may be read or intercepted by others, even if there is a special notice that a particular transmission is encrypted."	
								yes (incl. videostreams)	
								yes (incl. videostreams)	
								Yes for small meeting rooms of 4 people. No for large rooms (5 to 12 people). See their privacy policy security section	

Desktop update frequency[2]	Mobile update frequency[2]	Potential Information Security Risks5	Recent security incidents[3]
4 times over the last 3 months,	4 times during the last 3 months,	to be considered. High probability due to recent security vulnerabilities	Zoombombing
approx 4 updates/month	approx 4 updates/month	to be considered.	
not available	not available	to be considered	
not available	not available	to be considered	
once in every few months, latest March 2020		to be considered	
no separate Hangouts meet product update list available		to be considered	

last updated Jan 31 2020		SLA with EP applies	
		SLA with EP applies	
		SLA with EP applies	
4 times over the last year		To be considered. European Commission assessment applies	
2-3 times/month	once in every few months	To be considered. European Commission assessment applies	
no history of updates available, latest update April 2020		To be considered	
3 times over the last month, now BBB 2.2.5.		To be considered	
		To be considered	
3 system updates over the last year	2 system updates over the last year	To be considered	

Assessment of videoconference and webinar tools for the EDPS

Background

With the spread of the Covid-19 pandemic, organisations are no longer able to act and work in physical proximity and are unable to organise in-person meetings. Consequently, there is a critical business need for secure audio/video conference and webinar solutions (hereinafter "VC") which allow for reliable communications online, in compliance with applicable data protection rules.

In this context, the EDPS is looking for viable solutions, which could integrate effectiveness, cost sustainability and compliance with data protection and security requirements.

Purpose

The Technology and Privacy (TP) unit was tasked with exploring and finding adequate tools for EDPS use cases. This note serves to document the ongoing efforts to identify viable solutions in the short term for use with external participants.

This document lists the use cases and their requirements. It features a table with a shortlist of tools with their features and their ability to support those use cases. For each and every use case, a conclusion is drawn as to the best supporting tool to be submitted to tests.

For the medium-long term, other solutions could be assessed more in detail due to rapidly evolving changes in the VC tools landscape as well as to possible different EDPS resource availability and priorities.

Scope

This section identifies what is considered in and out of scope for this assessment.

Includes ("IN" Scope):

- Methodology for quick assessment
- Immediate use cases (for 2020) and their requirements
- Pre-selection of tools
- Basic assessment of pre-selected solutions against use case requirements

Excludes ("OUT" Scope)

- Tools part of unified communications offer from EP, solely for internal use (Jabber with Multipoints)
- Detailed assessments of available solutions on the market
- Lines to take and data protection guidance to other EUI for videoconference and webinar tools
- Considerations for satisfying EDPS VC needs beyond 2020, subject to a separate analysis of the overall organisational IT needs.

Methodology

TP has inventoried a large number of possible VC solutions[1] based on their features and compliance with data protection and security requirements. In parallel, we identified use cases and relevant functional requirements. Due to the necessity of identifying and testing a limited number of tools, we made a shortlist based on some key criteria, including:

[1] They are reported here: https://saas.fabasoft.com/edps/mx/COO.6515.100.2.396786

- the potential number of participants in meetings;
- features provided for different use cases, with a distinction between tools geared towards conducting meetings (all participants able and expected to interact in small number videoconferences) versus webinars (where a few presenters present to large audiences, with recording capabilities)
- the expected level of confidentiality and data protection assurance;
- the level of institutional control on the solution;
- the current availability of VC tools within the offer from the EP in the context of the Service Level Agreement (SLA) we signed with them;
- the existence of turnkey solutions as fall-back options in case the others turn out inadequate.

Further info on some of the discarded solutions can be found in Annex I

Use cases and their requirements

The main use cases identified for online meetings and webinars the EDPS organises are the following:

1. **Work meetings** organised by EDPS staff, with staff from other EUIs or external stakeholders and a limited number of participants. This includes meetings of the **Supervision Coordination Groups (SCGs)** from EDPS and national DPAs.

a. The **number of participants is limited** (up to 25, with the exception of 50 for SCGs)
b. Confidentiality requirement: up to very high
c. Need to connect also from within the EUIs and national administrations' infrastructure, which entails the availability of a web client (usually not possible to install ad hoc apps)
d. Usually no recording

2. **DPO meetings**

a. The number of participants is high (70-120, limiting the number to 2 per EUI)
b. Confidentiality requirements: high, since DPOs will probably share concerns and pose questions from which EUI legal compliance (or lack of) could be inferred.
c. Need to connect also from within the EUIs infrastructure, which entails the availability of a web client (usually not possible to install ad hoc apps)
d. Possible recording

3. **Training sessions and online events (e.g. IPEN and international organisations workshops)**

a. The number of participants is high (above 50, no upper limit yet 300 is acceptable)
b. Confidentiality requirements: none or low. We might though need some moderation features, e.g. in chats.
c. Need to support a large variety of clients, at least the most popular browsers
d. Recording

Other common requirements:

e) Data protection compliance. Relevant organisational risks, incl. reputational ones, need considering, too.
f) Information Security risks, such as exposure of EDPS information, risks related to inherent technical vulnerabilities, integrity and availability.
g) Screen/content sharing needed to show presentations
h) Interaction with speakers requires "raise hand" function and/or chat.
i) Client bandwidth requirements. Ideally, people with low quality Internet connections should be able to join the events, too.
j) Cost

Pre-selected tools

The pre-selected tools are:

- Webmeeting. The tool is within the European Parliament IT service offer. We can use it in the context of the EDPS SLA with the European Parliament for up to 50 participants at no extra cost.
- Cisco Webex Meeting. The tool is within the European Parliament IT service offer. We can use it in the context of EDPS SLA with the European Parliament at a very small cost per minute (0.0158 EUR). The EP has signed with British Telecom (BT) a specific contract within the inter-institutional framework contract DI/07540 (WACS II), managed by EC DIGIT and providing web and audio conferencing services, including Cisco Webex Meeting. While the WACS II framework contract is set to expire in November 2020, we do not currently know the end date of the specific contract of the Parliament.
- Big Blue Button (BBB). This is an open source solution used by many educational institutions. Currently, software issues involving outdated browsers prevent connections to BBB from EC and EP networks. A solution should be available in June 2020. Then, BBB can be deployed by a cloud service provider and managed by EDPS staff, or used as a Software as a Service (SaaS) in the offer from a service provider.

Tools features and requirements vs use cases

1. **Work meetings with limited number participants (including SCGs)**

Requirement	WebMeeting	Webex	BBB
a) number of participants	Yes[2]	Yes	Yes
b) confidentiality	Yes	Partial[3]	Partial[4]
c) Connection possible via web browsers	Yes	Yes	Partial[5]

2. **DPO meetings**

Requirement	WebMeeting	Webex	BBB
a) number of participants	No	Yes	Partial[6]
b) confidentiality	Yes	Partial	Partial
c) Connection possible via web browsers	Yes	Yes	No

[2] For SCGs, usually with more than 25 participants a special configuration needs to be requested to the EP. Request is ongoing. We do not expect high availability, though, so far.
[3] The current security assessment identifies possible risks of unauthorised access and eavesdropping, due to lack of end-to-end encryption (which is though common to most of the VC services due to technical limitations) but mainly to localisation of servers outside the EU/EEA.
[4] Depending on the location of the server and to assurances from the service provider. See also footnote 3 for lack of end-to-end encryption. End-to server encryption is supported, though. Until planned update for EUIs corporate Firefox version, only phone dial in and slide sharing is available for users on EUI corporate devices.

d) Recording	No	Yes	Yes

3. Training sessions and online events

Requirement	WebMeeting	Webex	BBB
a) number of participants	No	Yes	Yes
b) confidentiality	Yes	Yes	Yes
c) Connection possible via web browsers	Yes	Yes	Yes[7]
d) Recording	No	Yes	Yes

Shared requirements

Requirement	WebMeeting	Webex	BBB
e) Data protection compliance	Yes, based on EP statement	To be completed[8]	Yes, yet provider-dependent
f) Info Security risks	Yes	Yes	To be defined
g) Screen/content sharing	Yes	Yes	Yes
h) Interaction with speakers requires "raise hand" function and/or chat	Chat No raise hand	Yes	Yes
i) minimum bandwidth required	2 Mbit/s, or only audio	0.7 Mbit/s (content + only presenter video)	1 Mbit/s recommended
j) Cost	No additional cost	Low per minute cost	use-dependent or approx. 500 EUR/month for hosted solutions

Data protection compliance for pre-selected tools

- **WebMeeting**.
  The tool is installed in the EP's data centre and the EP recommends it for confidential meetings with external people. The EP offers a WebMeeting data protection statement, which provides a good level of assurance. So far, we have no more information on the contractual agreements pinpointing this service.

- **Cisco Webex Meeting**

[8] See section on Data protection compliance for pre-selected tools.

The framework contract DI/07540 (WACS II) with British Telecom (BT), including Cisco Webex Meetings, was amended to integrate data protection contractual clauses as provided by Article 29 (3), of Regulation 2018/1725. On the other hand, having a look at the general privacy policies of Cisco (acting as a sub-contractor to BT) we are not completely reassured that they fully comply with EU data protection law (e.g. possible transfers of personal data to third parties, server locations outside EU/EEA). A joint action by the EDPS and EP DPOs is ongoing to ascertain that Cisco provides adequate safeguards and guarantees as sub-processor. End-to server encryption is available (protection against third party eavesdropping, but for server administrators).

- **Big Blue Button**.
  We are looking for a solution where the BBB solution be deployed within the EU/EEA. The ability to manage our BBB server might enable us higher level of data protection compliance, yet it entails a great amount of specialized human and technical resources in order to meet best practices in professional IT management and IT security requirements. If used by a SaaS service provider, it will depend on their data protection practices and their level of IT management / IT security posture. End-to server encryption is available (protection against third party eavesdropping, but for server administrators).

Suggested options to be submitted to tests (to date)

a) **Work meetings with limited number participants (including SCGs):** Webmeeting

b) **DPO meetings:** Webex Meeting

c) **Training sessions and online events:** BBB for the IPEN workshop, with WebEx as fallback.

Annex I

Solutions we have tested and discarded include:

- Zoom.us, currently the most popular videoconferencing on the market but with a history of security flaws, discarded on advice of CERT-EU pending at least a 90 day period during which they intend to achieve full compliance with security and data protection requirements, providing end-to-end encryption (E2E) and possibility to choose the data centre used for the cloud hosting, among many other security and trust-enhancing measures
- GoToWebinar.com, the most popular webinar solution provided by US company LogMeIn, provides easy-to-use interface, but was found lacking configuration options for compliance with data protection requirements, especially considering that they just introduced automatic transcription, with unclear opt-in opt-out options in the cloud
- Whereby.com, is a small scale videoconferencing solution provided by Norwegian company, limited to max 50 participants with 12 video connections at the same time
- Pexip.com, is the Norwegian videoconferencing solution the Council uses to connect other solutions used in Member States (notably providing bridges to Microsoft and Goole solutions) potentially sharing personal data with these third party services
- Tixeo.com is the secure videoconferencing solution recommended by the FR DPA, as the only solution on the market we are aware of that is certified by a Cybersecurity agency (the FR ANSSI in 2017), discarded as requiring installation of native client by all parties
- Forum Vision is the hosted online platform proposed by event organisation firm Forum Europe, which is geared towards big online conferences resembling traditional in-person conference settings, integrating the startup hopin.to solution, using Amazon Web Services (AWS) in the UK and US to deliver high quality events at a relatively high price. We believe its price does not justify 2020 immediate needs yet could be considered as an option for possible future big events entailing wider functional requirements and organisational support, subject to further assessment of its security and data protection stand.

In conclusion, we found most of the solutions currently available mainly lack either data protection by design and by default considerations, or the flexibility we need to deploy on EP infrastructure/in browser.

Preliminary privacy assessment of Zoom as online conferencing tool

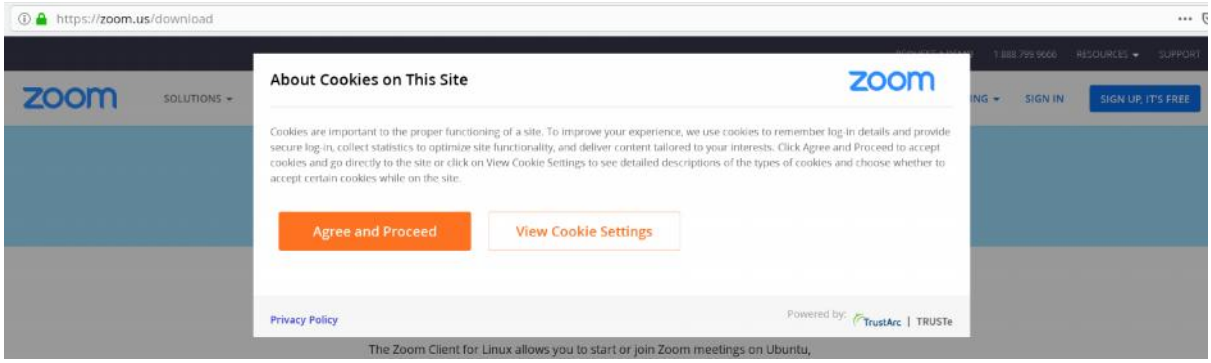
IT Policy Unit has been requested on 15 February a privacy assessment on two tools for podcasting with remotely connected speakers: Jitsi and Zoom.

IT Policy Unit sent a feasibility study on 21 February outlining the strong points and weaknesses of the tools proposed.

On 25 February IT Policy Unit was informed that the EDPS has contracted a "Pro" subscription plan of the service offered by Zoom. IT Policy Unit staff conducted some tests with the EDPS account.

Results of the tests

When joining a meeting using a URL provided by the organizer, the browser shows the participant a modal notice (cookie wall) with the available options.



Even before the participants has made any decisions, some cookies and HTML5 local storage are set on their devices. Some of those cookies (e.g. Google Analytics) are not exempted from the requirement to obtain previous informed consent.

This behaviour does not follow the recommendation 3 of the EDPS web services guidelines.

The default configuration ("Agree and proceed") is to accept all types of cookies which are classified as advertising, web functional and required). To limit the cookies to the required ones it is necessary to go into the option "View Cookie Settings".

This behaviour does not follow the recommendation 18 of the EDPS web services guidelines.

Google Analytics cookies are kept even if the participant limits the cookies to the required ones.

Current EDPS account of the Zoom service is set up so only local recording is allowed. Recording on the cloud service provided by Zoom is disabled.

Once the meeting has finished the service automatically starts the conversion of the collected data into a set of five files containing the video, audio and chat data of the meeting.

Using the user interface we could not found any recording or chat message related to previous test meetings.

Legal document assessment

This section contains a list of flaws detected on legal documents available at Zoom's website.

Privacy Policy

- The document does not make clear when Zoom acts as data controller or as data processor.

  The policy states that "*We may collect, either as Controller or Processor, the following categories of Personal Data about you when you use or otherwise interact with our Service:...*" and "*We collect and retain, generally as a Processor and in order to provide the Services, Personal Data and other information you upload, provide, or create while using the Service*"

- The EDPS should inform to all participants that, as the policy states: "*All messages and content you share in a meeting, including Personal Data about you or others, will be available to all other participants in that meeting.*".

- There is no information on the specific retention periods.

- The policy states that "If you use a feature of the Products that allows for Recordings (defined below), we collect information from you that you provide in connection with such use and through such Recordings, to the extent you provide it to us. This information may include Personal Data, if you provide us with Personal Data.". The policy further states that "Any person and/or entity who makes a Recording of a meeting or webinar shall be the data controller of that Recording, and Zoom will be the data processor with respect to the Recording.". It is clear that Zoom processes personal data in and related to recordings for their own purposes. They are not mere processor, but (joint) controllers for that processing.

- Zoom products do not support Do Not Track requests, which means that they collect information about visitors online activity both while they are using the Products and after they leave Zoom's websites.

  This behaviour does not follow the recommendation 23 of the EDPS web services guidelines.

Processing addedum

- The Processing addendum refers to compliance with Directive 95/46 and the GDPR.

- Use of sub-processors based outside of the EEA (mostly US), including in countries without an adequacy decision. Incomplete list of sub-processors[1] (e.g. Facebook, Google Analytics, PayPal...). Incoherence between provisions on sub-processors in the Processing addendum and the list of sub-processors, which limits the notification of the controller of any new sub-processors "*to the extent required under contractual agreement, along with posting such updates here*". This raises doubts on the compliance with Art. 29(2) of Regulation 2018/1725 (and Art. 28(2) of the GDPR), is the controller has not signed the Processing addendum with Zoom.

- EXHIBIT A. (Details of Processing) to the Processing addendum is not in line with the details provided for in the Privacy Policy document (e.g. types of personal data processed)

- EXHIBIT B. (Standard Contractual Clauses) to the Processing addendum is not in line with the details provided for in the Privacy Policy document (e.g. types of personal data processed).

[1] https://zoom.us/subprocessors

- Section 6 (Transfers of Personal Data) does not prohibit onwards transfers of personal data by the processor or sub-processors.
- Paragraph 7.1. of the Processing addendum limits the notification of the Controller of data subjects requests to the extent permitted by law. As the controller is the one ultimately responsible for fulfilling all controller's obligations (ensuring information and other data subject rights) and liable for any breach of those obligations. Therefore, in case the processor received and responds to data subject requests, the controller should be notified of the requests and the responses.
- Paragraph 8.1. of the Processing addendum states that the processor shall provide the controller with reasonable cooperation and assistance where necessary for Controller to comply with its obligations under the GDPR to conduct a data protection impact assessment and/or to demonstrate such compliance, provided that Controller does not otherwise have access to the relevant information. The assessment of that is reasonable is left to the processor. This limitation to what is reasonable is not in the GDPR (or Regulation 2018/1725).
- Paragraph 8.2. of the Processing addendum states that the processor shall provide the controller with reasonable cooperation and assistance with respect to Controller's cooperation and/or prior consultation with any Supervisory Authority, where necessary and where required by the GDPR. The assessment of that is reasonable is left to the processor. This limitation to what is reasonable is not in the GDPR (or Regulation 2018/1725).
- Paragraph 8.4. of the Processing addendum limits the controller's right to audit only to once per calendar year review of "*copies of certifications or reports demonstrating Processor's compliance with prevailing data security standards applicable to the Processing of Controller's Personal Data*".
- According to paragraph 8.5 of the Processing addendum in the event of a Personal Data Breach, Processor shall *"… take such steps as Processor in its sole discretion deems necessary and reasonable to remediate such violation (to the extent that remediation is within Processor's reasonable control)*". Thus, even though the controller is responsible for data breaches, it cannot give the processor any instruction on additional measures to mitigate the data breach if it deems that the measures taken by the processor are not enough. Paragraph 8.6. of the Processing addendum limits the cooperation and assistance to controller only to what is reasonable. The assessment of that is reasonable is left to the processor. This limitation to what is reasonable is not in the GDPR (or Regulation 2018/1725).

Cookie policy and consent management mechanism

- From this document, it is clear that Zoom is collecting data for their own purposes (e.g. for improving products and informing about Zoom's events and promotions and offers from third parties, personalised marketing communications). This collection of data using cookies and tracking technologies by Zoom and their third-party service providers is also set out in the privacy policy.
- There is no information on the duration of cookies and the retention period of the collected data.

Terms of service

- Section 3.c (Recordings) of the terms of service states that "You are responsible for compliance will all recording laws. The host can choose to record Zoom meetings and Webinars. By using the Services, you are giving Zoom consent to store recordings for any or all Zoom meetings or webinars that you join, if such recordings are stored in our systems. You will receive a notification (visual or otherwise) when recording is enabled. If you do not consent to being recorded, you can choose to leave the meeting or webinar.". Use of the Services is subject to Zoom's privacy policy. As privacy policy and other policies are incorporated into the Terms of service, by consenting to recording host and meeting participants are consenting to Zoom's processing of the personal data in and related to recordings for their own purposes.

  This can be mitigated by signing a separate written agreement with Zoom governing our use of the service, since in line with paragraph 20.3 (General provisions) of the terms of service such separate agreement would take precedence over Zoom's terms of service, privacy policy etc.