Risk Scenario ref.			Risk Scenario Components					(August 2020)
R.S. Pri.	R.S. Cat.	Risk Scenario ref.	Threat actor	Threat Type	Event	Asset/Resources	Time	Risk description
1	Data protection	**Cisco WebEx licensing, billing and analytic users data sent to US.**	External	External requirem.	Considering the international dimension of the Cisco company for infrastructural or legal reasons the user private data supplied to Cisco by the Court for licensing and billing processes is currently sent to the US data centre.	Primary assets: Court's reputation, Court WebEx users/data subjects private data transferred to Cisco US. Secondary assets: Court's videoconference infrastructure.	Duration of the event: The whole period of validity of the Cisco contract. Timing (when it occur): The whole period of validity of the Cisco contract. Detection: contractual indications, Cisco information.	Billing and analytical data containing also the WebEx users personal data, are sent to the US. This is currently not compliant with the Regulation (EU) 2018/1725 (EUIs GDPR) since the Schrems II judgment of the Court of Justice of the EU in July 2020.
2	Data protection	**Third country authority request to access WebEx users private data in EU.**	External	External requirem.	Third country authorities can request Cisco the access to the Court's WebEx data in accordance with provisions defined in that country's laws.	Primary assets: Court's reputation, Court's sensitive data, Court WebEx users/data subjects private data accessed. Secondary assets: Court's videoconference infrastructure.	Duration of the event: The whole period of validity of the Cisco contract. Timing (when it occur): The whole period of validity of the Cisco contract. Detection: very difficult.	A third country could enforce Cisco to transfer Court's WebEx sensitive information or Court WebEx user's private data to that country authority. (E.g. on the legal base of the US Cloud act or the Foreign intelligence surveillance act, Cisco could be forced to transfer Court sensitive data or private data to a US authority).
3	Organisational	**Unclear structure of the first Cisco contractual proposal also referring to online documents.**	External	Failure	Ineffective design of the contractual documents.	Contract.	Duration of the event: Contract validity period. Timing (when it occur): During the first contract definition phases. Detection: by the legal advisor and DPO.	Unclear structure of the first Cisco contractual proposal, with references to online documents.
4	Organisational	**Current Court's Cisco WebEx infrastructure partially obsolete and underdimensioned.**	Internal	Failure	The current Court's Cisco on premises infrastructure is no longer adequate to the teleworking necessity. Further the on premises Cisco WebEx Meeting will soon be in End of Support status.	**Primary assets:** Court's teleworking processes. **Secondary assets:** Court's video conferencing and infrastructure.	**Duration of the event** Until the Cisco infrastructure at the Court will not be upgraded. **Timing (when it occur)** The whole period of validity of the old Cisco contract. Detection: problem known.	Since the beginning of the extensive use of smart working and of the related technologies, the Cisco infrastructures and services on premises have proved not to be adequate to the new needs. Further, the Court on premises Cisco WebEx Meeting will soon be in End of Support status.

5	Data protection	**Cisco WebEx users data sent to UK.**	External	External requirem.	The data directly or indirectly produced by the Court's WebEx users could continue to be shipped also to the UK Cisco data centre after the 1 January 2021, even in case of no Brexit agreement.	Primary assets: Court WebEx users/data subjects private data transferred to Cisco UK.	Duration of the event: The whole period of validity of the Cisco contract. Timing (when it occur): The whole period of validity of the Cisco contract. Detection: contractual indications, Cisco information.	From 1 January 2021, should no EU/UK agreement be enacted, UK could be considered in GDPR terms as a third country. This could imply the prohibition to transfer Court's WebEx users private data to UK.
6	Organisational / Data protection	**Uninvited guest joins a video conferencing meeting.**	External	Malicious	Theft, disclosure of information communicated during a videoconference.	Primary assets: Court's reputation, Court's sensitive data, Court WebEx users/data subjects private data accessed. Secondary assets: Court's videoconference infrastructure.	Duration of the event: videoconferences. Timing (when it occur): Mismanaged videoconferences. Detection: possible by the videoconference host, guests or system administrators.	An uninvited guest could join a video conferencing meeting. This can happen, if a password is not required and the meeting ID can be discovered. The risk is higher if the videoconference host and the guests do not correctly manage the meeting information/link.
7	Cybersecurity	**New video conferencing systems vulnerabilities, specific malware and zero days attacks.**	External	Malicious	Attacks related with new vulnerabilities, threat actors and new techniques.	**Primary assets:** Court's sensitive information. **Secondary assets:** Court's Cisco infrasructure, Court's IT infrastructure.	**Duration of the even**t Whenever the Cisco services at the Court and on the Cloud will be in use. **Timing (when it occur)** The whole period of validity of the Cisco contract. **Detection:** can be difficult.	Continuous discovery of new video conferencing systems vulnerabilities, specific malware and zero days attacks.
8	Organistional	**Lack of ad hoc policy and procedures to establish which types of information can be processed on the cloud or on premises.**	Internal	Failure	The available range of video conferencing and unified communication services could lead users to use an inappropriate service with regards to the type of information processed.	**Primary assets:** Court's sensitive information, Court WebEx users/data subjects private data accessed. **Secondary assets:** Curia Cisco infrastructure. Cloud Cisco infrastructure.	**Duration of the event** Whenever the Cisco services at the Court and on the Cloud will be in use**.** **Timing (when it occur)** The whole period of validity of the Cisco contract**.** **Detection:** can be difficult.	A lack of ad hoc policy (e.g. acceptable use policy) and procedures, which should be aligned with the Court's corporate policy, are necessary to define which types of information can be processed on the cloud or on premises and under which conditions.

9	Organisational / Data protection	**Host inappropriate video conferencing system choice.**	Internal	Failure	Use of the cloud video conferencing system for particularly sensitive Court information or private data.	Primary assets: Court's reputation, Court's sensitive data, Court WebEx users/data subjects' private data. Secondary assets: Court's videoconference infrastructure.	Duration of the event: video conference time. Timing (when it occur): Mismanaged videoconferences. Detection: possible by the videoconference host or guests.	The Court video conferencing infrastructure will be made of two parts, one on premises and another on the cloud. The on premises infrastructure will ensure the highest level of security and privacy. The use of one or the other service should strictly be dependent from the type of information treated during the video conference. Should a host use the cloud service for Court sensitive information or sensitive private data, a lower level of security would be provided.
10	Data protection	**Lack of clarity over location of EU data, both at rest and in transit**	External	Failure	Because Cisco has not yet adapted its processes to be fully compliant with the latest EU legal constraints, the location of EU data at rest and in transit is not clearly defined.	Primary assets: Court's reputation, Court's sensitive data, Court WebEx users/data subjects private data accessed. Secondary assets: Court's videoconference infrastructure.	Duration of the event: Until Cisco will not adapt its data management processes. Timing (when it occur): Whenever the Cort's data is not processed accorning to the latest EU legal constraints. Detection: difficult.	The Court's Schrems II judgment and the Brexit outcome will affect the Cisco EU data management and storage processes. Currently Cisco have not yet adapted its processes to be fully compliant with the latest EU legal constraints. For this reason, personal data breaches cannot be excluded.
11	Data protection	**Billing, analytics and video conferencing generated data used by Cisco for profiling the Court Cisco services users.**	External	Failure	Court video conferencing data used for unforeseen purposes (e.g. users profiling, etc.)	Primary assets: Court WebEx users/data subjects.	Duration of the event: Contract validity period. Timing (when it occur): During the first contract definition phases. Detection: difficult.	All type of data related with the Cisco video conferencing services and managed by Cisco could be used for purposes not foreseen by the Court of Justice of EU.
12	Organisational / Data protection	**Record of processing activities and notice preparation.**	Internal	Failure	Preparation of the regulation 2018/1725 record of processing activities.	**Primary assets:** Data subjects rights, Court compliance with the regulation 2018/1725.	**Duration of the event** Whenever the processing activities related with the Cisco services will be undertaken. **Timing (when it occur)** The whole period of validity of the Cisco contract. **Detection**: Easy.	As stated by article 31 of the regulation (EU) 2018/1725, the controller of the processing activities related with the Cisco services shall maintain a record of the processing and a notice which will be kept in the DPO registry records.

13	Organistional	**Unforeseen data transfer from the Court to Cisco.**	Internal	Error	Because of unforeseen human errors, private data could be sent to Cisco.	**Primary assets:** **Court WebEx users/data subjects private data.** **Secondary assets:** **Court's IT infrastructure.**	**Duration of the event:** during the services availability. **Timing** (when it occur): The whole period of validity of the Cisco contract. **Detection:** can be difficult.	The activation or blocking of Cisco licenses is a process that will have to be done from the signature of the contract and will continue for the duration of the contract. The automatic process involves sending the license activation information (pseudonymized email address and pseudonymized name) to Cisco. Depending on the method and protocol used there can be human mistakes involving the sending of unnecessary information to Cisco. This event could constitute a data breach (GDPR).
14	Cybersecurity	Court's teleworking infrastructure attacks.	External	Malicious	External threat actors trying to overcome the Court's defenses between the remote teleworkers and the Court internal infrastructure.	Primary assets: Court's reputation, Court's sensitive data, Court users/data subjects' private data. Secondary assets: Court's ITC infrastructure, Court's remote laptops, Court's protected communication channels (VPN, etc.).	Duration of the event: during the whole period of teleworking. Timing (when it occur): attempts of this type of attack occur continuously. Detection: several detections systems.	The Court internal and externa infrastructure surface is, as any other EU Institution, subject to continuous attacks attempts. For this reason the measures to protect the teleworking clients, the related communications channels as the rest of the Court infrastructure are essential.

	Risk scenario first assessment (August 2020)							Residual risks scenario assessment (December 2020)	
Existing Controls	**Threat description**	**Threat level**	**Vulnerability descr.**	**Vulner. Level**	**Impact descr.**	**Impatc level**	**First estimation of the risk**	**Proposed / implemented measures**	**Resudal risk**
Specific controls not yet implemented.	Transferring some Court's WebEx users personal data to US could have an impact on the data subject rights.	**3**	Specific technical solutions and contractual clauses not yet implemented. Contract not yet signed (08/2020).	**5**	Possible impact to the data subjects and lack of EUIs GDPR compliance implication for the DTI (controller). The data subject rights could not be respected because currently US do not ensures an adequate level of protection.	**2**	**30**	Technical controls. (1) The Name, surname and the email address of the WebEx users sent for billing purposes to Cisco US are now pseudonymized. (2) From 2021 (date tbd) all types of data will only be sent to Europe Cisco data centres. Supplemental contractual measures. (3) The Court reserves the right to terminate the contract if CISCO does not fulfill the Court's requirements by the end of Year 2021.	**T=3 V=2 I=2 R=12**
Specific controls not yet implemented.	A third country authority could ask Cisco to have access to the Court's WebEx private data stored in EU.	**2**	Specific measures not yet implemented. Contract not yet signed (08/2020).	**4**	The data subject rights could not be respected because a third country by GDPR definition do not ensures an adequate level of protection.	**3**	**24**	Supplemental contractual measures. (1) A supplemental contractual clause has been added to the contract stating that any request for access from a public authority can only be given after written authorization from the Court of Justice of the EU. Security controls. (2) A correct use of the Court on premises videoconference infrastructure would imply no transfer of WebEx users data outside the Court of Justice of EU. (3) The new Jabber video feature, allowing two Court internal users to initiate a Jabber internal videoconference will reduce the use of WebEx videoconferences.(4) The introduction of the WebEx meeting Pro end to end encryption between the videoconference endpoints including external participants, reduce drastically the user generated information available or accessible to Cisco.	**T=2 V=1 I=3 R=6**
Court Legal Advisor and the Data Protection Officer.	The first contractual proposal done by Cisco was not clear and did not contain all the necessary clauses necessary to ensure the GDPR compliance.	**2**	Inadequate contract proposal.	**3**	Possible repercussions on GDPR compliance.	**3**	**18**	Supplemental contractual measures. (1) The final contract will include all the necessary documents as annexes. (2) Should any contract external condition be contradictory, the contract will always prevail.	**T=1 V=1 I=3 R=3**
The Cisco contract revision and the new Cisco services testing have already started.	Contract renewal mismanagement.	**1**	Lack of adequate video conferencing contract and services.	**4**	Because of the Court adoption of the teleworking for all the employees since the beginning of the pandemic period, many Court's important processes could be impacted.	**4**	**16**	Contractual measures. (1) The signature of a new contract to cover all the Cisco services. Technical controls. (2) The adoption of new Cisco technologies on premises and on the cloud to replace obsolete services and to adapt the infrastructure to the new needs.	**T=1 V=1 I=4 R=4**

Specific controls not yet implemented.	Transferring Court WebEx users personal data to UK could have an impact on the data subject rights.	**2**	Specific technical solutions and contractual clauses not yet implemented. The risk will not occur before 01/01/2021.	**3**	Possible low impact to the data subjects and lack of EUIs GDPR compliance implication for the DTI (controller).	**2**	**12**	Technical controls. (1) From summer 2021 the videoconference data will only be sent in the European Union data centres. Should UK be considered a third country the London data centre would be excluded. (2) The introduction of the WebEx meeting Pro end to end encryption between the videoconference endpoints including external participants, reduce drastically the user generated information available or accessible to Cisco. (3) The new Jabber video feature, allowing two Court internal users to initiate a Jabber internal videoconference will reduce the use of WebEx videoconferences. Supplemental contractual measures. (4) The Court reserves the right to terminate the contract if CISCO does not fulfill the Court's requirements by the end of Year 2021.	**T=2 V=1 I=2 R=4**
Data encryption for meetings, transmission and storage. User authentication.	Malicous actor would join a videoconference to listen in on the conversation or for other malicious purposes.	**1**	Host/guests video conference mismanagement. Lack of users security measures awareness.	**3**	Possible impact to the video conference participants (data subjects). Possible leaking of sensitive information.	**4**	**12**	Technical controls. (1) Proper use of the existing security measures (e.g. the host should require passwords; all the participants should verify attendees, check meeting links, keep confidentiality, report suspicious activity). (2) A Pre-access admission will be implemented to allow the organiser to verify if the participant were all invited. (3) Improve users' security awareness by planning specific awareness raising campaigns for Court users. (3) Continuous vulnerabilities analysis and related patch management. (4) Videoconferencing specific policy and ad hoc procedures definition.	**T=1 V=2 I=4 R=8**
Court and Cisco cloud existing security measures (end point, perimetral, etc.).	Threat actors exploiting the vulnerabilities.	**1**	Many vulnerabilities are discovered regularly.	**3**	Many different impacts are possible depending the type of attack.	**4**	**12**	Cisco researchers and other external researchers detect new vulnerabilities on a weekly basis. Thanks to the Cisco security investments, new patches are issued regularly and promptly. The Court's processes related with vulnerabilities analysis, patch management and continuous revision of the security measures can greatly reduce the risks of this category.	**T=1 V=1 I=4 R=4**
Specific controls are not yet implemented.	The users could use an inappropriate service with regards to the type of information processed.	**2**	Lack of an ad hoc policy and related procedures	**2**	Possible impact to the Court or to the video conference participants (data subjects). Possible leaking of sensitive information.	**3**	**12**	Technical controls. (1) Preparation of an ad hoc policy and related procedures /guidelines should be communicated to the Cisco services users. (2) Video Mesh Private meeting option soon availble. (3) The new Jabber video feature, allowing two Court internal users to initiate a Jabber internal videoconference will reduce the use of WebEx videoconferences.	**T=1 V=1 I=3 R=3**

Specific controls are not yet implemented because the services are not yet in production.	Video conference inappropriate service chosen by the host in relation to the information treated.	**1**	Host video conference mismanagement. Lack of users security measures awareness.	**3**	Possible impact to the Court or to the video conference participants (data subjects). Possible leaking of sensitive information.	**3**	**9**	Technical controls: (1) Video Mesh Private meeting option, soon availble, could avoid unintentional errors. (2) The introduction of the WebEx meeting Pro end to end encryption between the videoconference endpoints including external participants, reduce drastically the user generated information available or accessible by Cisco. Test will be done to check if this security measure can be always active and deactivated only when chosen by the videoconference organiser (e.g. to record the videoconference). (3) The new Jabber video feature, allowing two Court internal users to initiate a Jabber internal videoconference will reduce the use of WebEx videoconferences. (4) Improve users' security awareness by planning specific awareness raising campaigns for the Court video conferencing users. (5) Videoconferencing specific policy and ad hoc procedures definition.	**T=1 V=1 I=3 R=3**
Specific controls not yet implemented.	Because the localization of the EU users data is not clear, data subjects breaches cannot be excluded.	**1**	Specific measures not yet implemented. Contract not yet signed (08/2020).	**3**	Possible low impact to the data subjects and lack of EUIs GDPR compliance implication for the controller.	**3**	**9**	Technical controls. (1) From summer 2021 the videoconference data will only be sent in the European Union data centres. Should UK be considered a third country the London data centre would be excluded. Supplemental contractual measures. (2) The introduction of the WebEx meeting Pro end to end encryption between the videoconference endpoints including external participants, reduce drastically the user generated information available or accessible to Cisco. (3) The Court reserves the right to terminate the contract if CISCO does not fulfill the Court's requirements by the end of year 2021.	**T=1 V=1 I=3 R=3**
Specific controls are not yet implemented because the services are not yet in production.	Users information, related with the Cisco video conferencing system, used to profile them.	**1**	Inadequate contract proposal.	**3**	The profiling of the video conferencing users could imply data subjects and controller damages related with a lack of GDPR compliance.	**3**	**9**	Supplemental contractual measures. (1) No new unforeseen processing purpose can be implemented without a written agreement of the parts. Technical controls. (2) The introduction of the WebEx meeting Pro end to end encryption between the videoconference endpoints including external participants, reduce drastically the user generated information available or accessible to Cisco even for profiling purposes. (3) The new Jabber video feature, allowing two Court internal users to initiate a Jabber internal videoconference will reduce the use of WebEx videoconferences.	**T=1 V=1 I=3 R=3**
The documents have been planned and currently at the draft status.	Document not ready when necessary.	**2**	Document mismanagement.	**1**	Lack of compliance with the regulation (EU) 2018/1725.	**3**	**6**	The document will be ready before the contract signature.	**T=1 V=1 I=3 R=3**

Process not yet implemented.	The licensing process administrator could by mistake transfer more information then necessary to Cisco.	**1**	Lack of procedures.	**2**	Any personal data sent not stated in the register of processing activities will constitute a data protection breach and can potentially harm the data subject.	**3**	**6**	The preparation of ad hoc procedure will minimize this risk.	**T=1 V=1 I=3 R=3**
Internal infrastructure: Many type and layers of cybersecurity controls are implemented to protect and detect attacks attempts or intrusions. **External infrastructure:** Specific controls are implemented for the perimeter defense. Monitored via SIEM. **Teleworking laptops** Ad hoc controls are implemented which protect the information on the teleworking laptops and their communication with the Court. Monitored via SIEM.	Threat actors exploiting any vulnerability found in the whole Court's ITC infrastructure.	**2**	The Court vulnerability management process allows us to promptly detect new vulnerabilities.	**1**	The impact is stricly related to the type of attack.	**3**	**6**	A continuous risk based approach with threats and vulnerability management processes is used to continuously lower the new risks by improving the security controls.	**T=2 V=1 I=3 R=6**