	Risk	Mitigating measures Cisco	Mitigating measures Government	After measures
1	Loss of control due to lack of purpose limitation **5 categories of personal data**	Cisco has agreed to the revised DPA Amendment with specific processing purposes and further processing purposes as authorised data controller.	Make arrangements for the joint controllership between CIO-Rijk and participating government organisations.	Risk low: new DPA finalised 25 July 2025.
2	Loss of control due to **incorrect information** to data subjects: hyperlinks to terms & policies Cisco as data controller	Cisco will remove the incorrect references by the end of 2025 at the latest.	Inform data subjects until the end of 2025 that the links in the login screen are incorrect, that Cisco is processor for the government.	Risk low: Cisco removes incorrect references by the end of 2025.
3	Inability to exercise right of access to **Telemetry Data.**	Cisco will develop two Telemetry Data extraction tools by the end of 2025: 'live' access to the Telemetry Data in the Webex app, and access in the Control Hub for admins to the available historical Telemetry Data.	Inform data subjects how to submit a Data Subject Access Request and what to expect. Specify how data subjects can exercise their rights in the joint controllership arrangement between CIO-Rijk and participating government organisations.	Risk mitigated.
4	Inability to exercise right of access to Diagnostic Data: no access to **security logs**.	Cisco will provide access to available personal data in its security logs if Cisco is able to reliably connect the requester to the IP address in its logs. Cisco will inform data subjects of the existence and nature and retention period of these logs in response to a Data Subject Access Request.	Inform data subjects how to submit a Data Subject Access Request and what to expect. Make arrangements for the joint controllership between CIO-Rijk and participating government organisations.	Risk mitigated.
5	Loss of control due to lack of transparency on **Telemetry Data**.	Cisco publishes documentation of Telemetry Data since 1 July 2025. Cisco will further minimise the Telemetry Data collection in the new Webex apps that will be launched by the end of 2025	Inform users and admins how to access the live and historical telemetry data, and compare the outcomes with public documentation.	Risk mitigated.
6	Loss of control data transfer to third countries **Support Data.**	By 1 October 2025 Cisco will implement best-efforts ticket routing to its support engineers in the EU and defer tickets raised outside EEA business hours to the following day. Later, if requested by the BD and as agreed, Cisco will provide the BD with a dedicated support team consisting of engineers based solely in the EEA who are specifically trained and assigned to handle Client's support cases. The dedicated team will use a support ticketing system from an EU provider, or in-house by Cisco in the EU, Japan or another country with adequacy, but always without any controlling influence from, or transfer to, a company in the USA, Israel, the UK or a third country.	[BD] Disable the default access from Cisco engineers to the Control Hub (with access to logs). The BD has already requested the best efforts ticket routing solution, and aims to contract for the new EEA-based support solution.	Risk low: Cisco can implement the best effort ticket routing by 1 October 2025.
7	Loss of control data transfer to third countries Website Data **Login Websites** (rijksvideo.webex.com, user.webex.com and admin.webex.com)	Cisco has reduced the scope of the Akamai cookie from **webex.com** to **user.webex.com.** By the end of 2025, all processing via admin.webex.com, rijksvideo.webex.com and user.webex.com will take place exclusively in the EU. The revised DPA Amendment extends the agreed mitigating measures and protections to guest users.	Inform data subjects until the end of 2025 that the links in the login screen on rijksvideo.webex.com are incorrect, that Cisco is processor for the government.	Risk low: by the end of 2025, Cisco processes all Login Website data of admins and users as processor, and exclusively in the EU.
8	Loss of control data transfer to third countries **Account and Diagnostic Data**	Cisco will only engage sub-processors for the Rijksvideodienst by the end of 2025 that process the Account and Diagnostic Data within the EU territory, or, if earlier, the day after the EU US DPF becomes invalid. Cisco confirmed that its own employees do not have standing access to logs of the Rijksvideodienst outside support requests (after the BD has disabled the default access). By the end of 2025, Cisco will process the personal data related to the use of Slido exclusively within the EU.	[BD] Disable the default access from Cisco engineers to the administrator console (with access to logs). If necessary, the BD can enable ad-hoc access. [BD] Disable the Timer app if the EU US DPF becomes invalid.	Risk low: by the end of 2025, Cisco's sub-processors will process all personal data exclusively within the EU.
9	Loss of control data transfer to third countries **Content Data** (also as part of logs)	Cisco will make it possible from mid-2026 for hosts to turn off E2EE even during a meeting.	[BD] Turn on E2EE by default for all new and all existing users. Inform users that they can disable E2EE as hosts prior to a meeting. [BD] Disable use of media nodes outside the EU (even with E2EE as default). [BD] Disable the access from Cisco engineers to the administrator console (with access to logs). If necessary, the BD can enable ad-hoc access.	Risk mitigated if BD turns on E2EE by default.
10	Loss of control due to unspecified or excessive retention periods **Account, Content, and Support Data.**	CIO-Rijk may shorten Cisco's standard 60-day retention period of Account and Content Data after termination of the contract. Cisco will delete new support tickets after 15 months, if the BD follows the agreed procedure.	[BD] Implement policy that administrators must export and verify Account and Content Data before terminating the contract. [CIO Rijk] Determine the necessary retention period with Cisco after termination: for example 2 weeks. Ensure inactive accounts are removed by updating the list for the BD. Shorten the retention period for shared files, for example through labelling. [BD] Reconsider the necessity of the current 3,600-day period: this is Cisco's technical maximum. Clean up database with historical support tickets.	Risk low.
11	Loss of control due to unspecified or excessive retention periods: possibility that Cisco has **other logs** not visible for the government.	Cisco provided missing information on retention periods, and confirmed that there are no other logs.	N/A	Risk mitigated.
12	Loss of control due to unspecified or excessive retention periods and lack of transparency **cookies Login Websites** (rijksvideo.webex.com, user.webex.com, and admin.webex.com).	By 5 September 2025 Cisco will publish help articles with information about the retention periods of cookies for admin.webex.com, rijksvideo.webex.com and user.webex.com. Cisco will update its cookie consent manager by 30 October 2025 to include names, purposes and expiry date of the functional cookies. Cisco will (continue to) apply privacy by default to the cookies.	Warn admins not to consent to other than the required cookies.	Risk low: adequate documentation cookies by 30 October 2025.
13	Loss of control due to unspecified or excessive retention periods: cookies on the **publicly accessible websites** trustportal.cisco.com and on help.webex.com.	Cisco already documents names, purposes and expiry date of cookies set by help.webex.com and by the Cisco trust portal in its cookie consent manager. Cisco will (continue to) apply privacy by default to the cookies. Cisco will publish the retention period of the data it collects with these cookies on these 2 sites in Cisco's own web server log files before 1 January 2026.	Warn admins not to consent to other than the required cookies.	Risk low: adequate documentation cookies before 1 January 2026.
14	Loss of control **Content Data** due to deviation from central privacy settings (Android Feedback bug)	Cisco will launch a new version of the Webex apps before 1 January 2026 that will eliminate this bug.	Warn administrators and users not to provide Feedback to Cisco (not via the AI administrator console and not via Cisco's publicly accessible website).	Risk low: bug fixed before 1 January 2026.
15	Irritation and wasted time due to unsolicited commercial communications (**Account Data)**	N/A. Cisco does not send marketing communications to contacts, administrators or users, only if they actively sign up for newsletters.	N/A	No risk
16	*Chilling effects* through use of **Diagnostic Data** in Employee Monitoring System	N/A. Cisco does not display statistics or dashboards based on end-user 'online presence'.	[BD] Implement policies for what purposes the Diagnostic Data may be processed/how administrators should handle queries from participating organisations.	Risk low: only BD administrators can see the logs.

17	Loss of control **Content Data** due to unauthorised sharing of confidential files	Cisco protects against malware by filtering Content Data for viruses and malware through its ClamAV software.	Implement file sharing policies incl. collaboration with external participants and retention periods.	Risk low
18	Loss of control **Content and Diagnostic Data** through data transfer of images to third party (Giphy)		Centrally disable the use of Giphy.	Risk low
19	Loss of control **Content Data** through unnoticed microphone use		Use the option from Cisco to centrally disable use of the microphone for ultrasound detection.	Risk low
20	Loss of control due to application of unknown algorithms to **Content and Diagnostic Data** (profanity filter and priority selection of messages)	The 'Recommended Messages' algorithm is not available for EU users, Cisco will remove the option from the UI for EU users. Cisco will explore ways to improve the filter or offer an option to disable if the BD has complaints.	If the BD enables subtitling (with generative AI), keep track of problematic filtering and inform the BD.	Risk low