A tutte gli istituti scolastici clienti
Loro sedi

Oggetto: nota DPO piattaforme di web conference

È necessario tornare nuovamente sull'argomento Didattica a Distanza anche per fare chiarezza in relazione alle varie e continue richieste che riceviamo.

A tale scopo si precisa:

1. Già precedentemente al Provvedimento del Garante del 26 marzo avevo invitato alla cautela poiché si stava affrontando un evento straordinario non gestito correttamente dal ministero competente i quali uffici, solo dietro sollecito dello scrivente, con note diverse (anche dell'USR) hanno attenzionato la problematica del rispetto del GDPR sottolineando la piena e totalità responsabilità dei vari dirigenti scolastici;
2. Il citato Provvedimento del Garante non ha fatto altro che chiarire e confermare l'interpretazione che avevo dato sulla gestione della DAD tanto è che riporta testualmente:

"**Qualora la piattaforma prescelta comporti il trattamento di dati personali di studenti**, alunni o dei rispettivi genitori per conto della scuola o dell'università, il rapporto con il fornitore (quale responsabile del trattamento) **dovrà essere regolato con contratto o altro atto giuridico** (art. 28 del Regolamento).
E' il caso, ad esempio, **del registro elettronico**, **il cui fornitore** tratta i dati per conto della scuola e, pertanto, **assume il ruolo di responsabile del trattamento**. Le eventuali, ulteriori attività di didattica a distanza, talora fornite da alcuni registri elettronici, possono essere in alcuni casi già disciplinate nello stesso contratto di fornitura stipulato. Diversamente, **qualora il registro elettronico non consentisse videolezioni** o altre forme di interazione tra i docenti e gli studenti, potrebbe essere sufficiente – per non dover designare ulteriori responsabili del trattamento- **utilizzare servizi on line accessibili al pubblico e forniti direttamente agli utenti, con funzionalità di videoconferenza ad accesso riservato**. Alcuni di questi servizi sono, peraltro, **facilmente utilizzabili anche senza la necessaria creazione di un account da parte degli utenti**. **Laddove, invece, si ritenga necessario ricorrere a piattaforme più complesse e "generaliste", che non eroghino servizi rivolti esclusivamente alla didattica, si dovranno attivare, di default, i soli servizi strettamente necessari alla formazione, configurandoli in modo da minimizzare i dati personali da trattare, sia in fase di attivazione dei servizi, sia durante l'utilizzo degli stessi da parte di docenti e studenti (evitando, ad esempio, il ricorso a dati sulla geolocalizzazione, ovvero a sistemi di social login che, coinvolgendo soggetti terzi, comportano maggiori rischi e responsabilità).**

3. Appare evidente che necessita porre la massima attenzione sulla scelta delle varie piattaforme di didattica a distanza poiché siamo in presenza di un atto che ha valenza giuridica specifica, contrariamente alle varie circolari o mail inviate dal Ministero competente.
4. Appare oltremodo chiaro che nella scelta di cui sopra, fino a quando i vari fornitori dei registri elettronici non attiveranno e saranno funzionanti correttamente la DAD, ci si dovrà orientare verso applicativi che dovranno essere utilizzati esclusivamente per le videolezioni sincrone (tutti gli altri tool degli stessi applicativi dovranno essere disattivati onde evitare problematiche legate al non rispetto del GDPR).
5. A maggior ragione, gli applicativi e le estensioni di terze parti non dovranno essere scaricati ed utilizzati poiché gestiscono i dati che transitano nei loro server in maniera non chiara.

Via N. Colajanni (pal. Di Vincenzo) n°161 ⌘ 93100 Caltanissetta
☏ +39 0934542970 (4 linee r.a.) 🖷 +39 0934543418 infoline +39 3383801547
web site: www.studiolobrutto.eu 🖃 info@studiolobrutto.eu
www.cermedquality.eu 🖃 info@cermedquality.eu

6. Tutti i servizi on line fino ad adesso utilizzati al di fuori del registro elettronico dovranno essere disattivati nel momento in cui il fornitore del registro elettronico attiverà definitivamente la DAD.

Altresì, appare molto riduttivo essere interpellato tout court per sapere se una determinata piattaforma è valida oppure no. La valutazione necessita di avere a disposizione tutta la documentazione rilasciata dal fornitore del servizio comprese le varie policy con indicazione della collocazione dei server nei quali vengono conservati i dati e la tipologia di crittografia attuata.

Da oggi tutte le richieste dovranno transitare tramite mail dedicata che ricordo che è: rpd.privacy@gmail.com , altre richieste non saranno prese in considerazione se non confermata tramite mail. Tutto ciò Vi prego di non ritenerlo un appesantimento burocratico ma come una chiarezza nel fare transitare correttamente i vari quesiti.

Preciso anche, che lo scrivente ha nessun interesse nell'esprimere parere negativo su alcune piattaforme utilizzate. Ricordo che il ruolo del DPO è di imparzialità, di assenza di conflitto di interessi e, soprattutto, di garante del rispetto del GDPR e della normativa italiana vigente onde evitare applicazioni sanzionatorie da parte degli organi competenti a voi dirigenti scolastici.

Vi allego una nostra guida sulla scelta delle varie app di videoconferenza tralasciando ZOOM poiché Vi ho già inviato un protocollo per impostare le nuove misure di sicurezza e funzionalità.

Prof. Riccardo Lo Brutto
DPO esterno

Via N. Colajanni (pal. Di Vincenzo) n°161 ⌘ 93100 Caltanissetta
☏ +39 0934542970 (4 linee r.a.) 🖷 +39 0934543418 infoline +39 3383801547
web site: www.studiolobrutto.eu 🖃 info@studiolobrutto.eu
www.cermedquality.eu 🖃 info@cermedquality.eu

Jitsi

Jitsi è una soluzione di videoconferenza gratuita e open source di proprietà dell'azienda californiana 8×8. Si presenta come una soluzione bivalente: la si può scaricare e installare sul proprio server; oppure, in alternativa, la si può utilizzare mediante la più famosa e immediata versione "Jitsi Meet".

Jitsi è disponibile via Web, oppure come app per iOS e Android. L'app è ricca di funzionalità e il numero di partecipanti che si può avere in videochiamata è (teoricamente) illimitato. Oltre alle videochiamate "di gruppo", Jitsi supporta anche la condivisione dello schermo, lo streaming su YouTube e la possibilità di postare un video YouTube per tutto il gruppo.

È inoltre possibile integrare Jitsi con Slack (strumento per la comunicazione veloce aziendale) e utilizzarlo per comunicare con il proprio team o con i propri utenti.

Pur se in itinere per implementarla, al momento Jitsi non supporta ancora una crittografia completa end-to-end. Con Jitsi i video inviati al server vengono criptati, decriptati presso il server e poi di nuovo criptati quando vengono trasmessi agli altri partecipanti. Questo significa che chiunque controlli il server potrebbe potenzialmente carpire le chat; e qui la differenza tra Jitsi "on site" – con il controllo del flusso protetto e "centralizzato" sui server aziendali – e Jitsi Meet (su server Jitsi) è rilevante.

Sul proprio sito Web, Jitsi non usa mezzi termini per tracciare il solco che la divide dai competitors in materia di sicurezza e privacy, preferendo un approccio chiaro e poco tecnico-giuridico. Jitsi dichiara di aver sviluppato una piattaforma affidabile per i suoi utenti, definendo le sue videoconferenze "private by design", che potremmo tradurre come "riservate fin dalla progettazione", parafrasando un concetto che chi si occupa di privacy conosce molto bene, ossia la privacy by design.

Jitsi afferma che le "stanze" ove si tengono le "riunioni" vengono create al momento che il primo partecipante si unisce e vengono distrutte quando l'ultimo partecipante se ne va.

Inoltre, se qualcuno si unisce di nuovo alla stessa stanza, si crea una nuova riunione con lo stesso nome ma con nessun collegamento con una riunione "omonima" precedente. Il tutto per rendere i meeting più difficili "da raggiungere" per chi non conosce gli elementi chiave.

In ogni caso, Jitsi afferma che bisogna scegliere con cautela il nome della stanza, per evitare che con un nome semplice faccia imbattere l'utente in persone "non gradite". Per evitare di scegliere nomi banali che possano permettere l'accesso a chiunque, Jitsi suggerisce di avvalersi del proprio servizio di "generatore di nomi casuali per riunioni", che creerà dei "nomi-stanza" difficili da rintracciare (al pari di ciò che accade per un generatore di password).

Inoltre, se si punta a un meeting "blindato", Jitsi consiglia di impostare una password – oltre a un nome – da comunicare a tutti i partecipanti alla riunione. Per quanto attiene la moderazione delle stanze, Jitsi garantisce una moderazione "limitata" alla sola risoluzione di problemi tecnici, come ad esempio i problemi che potrebbero esserci con il microfono o con la disconnessione.

Come accennato Jitsi, al momento in cui si scrive, non utilizza una crittografia "end-to-end", bensì una crittografia di tipo "hop-by-hop", ove tutto ciò che si invia al server viene criptato, poi decriptato sul server, e infine criptato nuovamente per essere inviato a tutti coloro che devono riceverlo. E questo spiegherebbe anche l'utilizzo della "moderazione tecnica limitata" da parte di Jitsi.

Entrando nel dettaglio, Jitsi afferma che le sue riunioni possono operare in due modi: peer-to-peer (P2P), per le riunioni uno-a-uno e con audio e video criptati con protocolli DTLS-SRTP (che proteggono da intercettazioni e manomissioni); o tramite il Jitsi Videobridge (JVB). Secondo Jitsi, nel caso di riunioni "multiparty", tutto il traffico audio-video è ancora crittografato sulla rete (mediante i già citati protocolli DTLS-SRTP).

Nel caso delle riunioni multiparty i "pacchetti" vengono decrittati durante l'attraversamento di Jitsi Videobridge; tuttavia non vengono mai memorizzati in un archivio in maniera "persistente" poiché vengono cancellati una volta consegnati agli altri partecipanti della riunione. Jitsi dichiara di non richiedere agli utenti "by-default" di creare un account.

Al di là dell'indirizzo IP del partecipante – ovvero del numero di telefono nel caso di collegamento telefonico – qualsiasi altra informazione che gli utenti scelgano di inserire, come il nome, la foto profilo e l'indirizzo e-mail, è puramente opzionale e viene condivisa solo con gli altri partecipanti alla riunione. Informazioni che vengono distrutte, specifica Jitsi, al termine della riunione.

Stessa sorte "distruttiva" tocca agli altri dati, come le informazioni contenute nelle chat, o le statistiche degli speaker che vengono conservati per tutta la durata della riunione e poi distrutti al termine della stessa. Per quanto attiene le registrazioni, Jitsi dichiara di conservarle sui suoi server fino a quando non vengono caricate sul cloud indicato dall'utente (ad esempio Dropbox).

Cisco Webex

Anche la soluzione di videoconferenza della Cisco spicca per sicurezza e protezione dei dati personali.

Tale piattaforma di videoconferenza, che esiste da più di vent'anni, ed è una delle preferite per via della sua "attenzione" alla protezione dei dati perché Webex ha la reputazione di mantenere una solida sicurezza informatica. Cisco, la società madre, è famosa per essere leader nel settore dell'hardware di rete, del software e dei prodotti di sicurezza.

Per tracciare il solco con Jitsi, Webex offre una crittografia end-to-end; il suo utilizzo, tuttavia, limita le opzioni video più diffuse, tra cui la condivisione remota del computer e le sale riunioni personali.

Di base però Webex non utilizza una crittografia end-to-end, bensì una crittografia che vede "flussi multimediali" che fluiscono da un client ai server Cisco Webex, i quali vengono decrittati dopo aver attraversato i firewall Cisco Webex.

Anche la soluzione di videoconferenza della Cisco spicca per sicurezza e protezione dei dati personali.

Di base però Webex non utilizza una crittografia end-to-end, bensì una crittografia che vede "flussi multimediali" che fluiscono da un client ai server Cisco Webex, i quali vengono decrittati dopo aver attraversato i firewall Cisco Webex.

Cisco può quindi fornire registrazioni basate sulla rete, così da permettere che tutti i flussi multimediali possono essere registrati per riferimento futuro. Cisco Webex crittografa nuovamente il flusso multimediale prima di inviarlo ad altri client.

Tuttavia, se si richiede un livello di sicurezza più elevato, Cisco Webex fornisce anche la crittografia end-to-end. Con questa opzione, l'azienda non decritta i flussi multimediali. Inoltre, tutti i client Cisco Webex generano coppie di chiavi e inviano la chiave pubblica al client dell'host.

L'host genera una chiave simmetrica casuale utilizzando un CSPRNG (Cryptographically Strong Secure Pseudo-Random Number Generator), la crittografa utilizzando la chiave pubblica che il client invia per poi trasmettere la chiave simmetrica crittografata al client. Il traffico generato dai client viene crittografato utilizzando la chiave di sessione simmetrica.

In questo modo, il traffico non può essere decifrato dal server Cisco Webex. Questa opzione di crittografia end-to-end è disponibile per i Cisco Webex Meetings e per il supporto Cisco Webex.

Nella sua corposa privacy policy, Cisco Webex dichiara che il servizio consente agli utenti di connettersi istantaneamente in modo personale al pari di un "incontro faccia a faccia". Cisco dichiara che l'organizzatore ha la possibilità di registrare le riunioni, mentre tutti gli utenti hanno la possibilità di caricare e conservare i file condivisi durante e al di fuori delle riunioni.

Infine, Cisco dichiara che l'organizzatore del meeting, nel caso voglia registrare la riunione, deve informare gli utenti della sua "intenzione". Se l'organizzatore del meeting sceglie di non registrare la riunione, la stessa verrà cancellata immediatamente dopo la conclusione della stessa.

Teams

Anche la piattaforma di videoconferenza di Microsoft, Teams, è degna di nota quando si parla di sicurezza e di privacy.

Microsoft dichiara di offrire una varietà di controlli sulla privacy e sulla sicurezza per consentire agli utenti di gestire chi partecipa alle riunioni e chi ha accesso alle informazioni sulle stesse**.**

Ad esempio, è l'utente "organizzatore" a decidere chi dall'esterno della propria azienda può partecipare direttamente alle riunioni e chi deve aspettare in attesa che qualcuno lo "faccia entrare". L'organizzatore può anche rimuovere i partecipanti durante una riunione nonché controllare quali partecipanti alla riunione possono presentare i contenuti. E con l'accesso degli ospiti, è possibile aggiungere persone esterne alla propria azienda, mantenendo comunque il controllo della situazione.

La moderazione da parte di Microsoft consente di controllare chi è o meno autorizzato a pubblicare e condividere contenuti.

Inoltre, Microsoft dichiara di utilizzare un'Intelligenza Artificiale avanzata per controllare le chat e prevenire comportamenti negativi come il bullismo e le molestie. Microsoft prosegue dichiarando che quando si registra una riunione, tutti i partecipanti vengono avvisati quando inizia una registrazione. Le registrazioni sono disponibili solo per i partecipanti alla call o per le persone invitate alla riunione. E le registrazioni sono conservate in un archivio controllato e protetto da permessi e crittografia.

A differenza di Jitsi e del suo private-by-design, Microsoft dichiara di proteggere la privacy dei propri utenti by-design. L'approccio di Microsoft alla privacy – dichiara l'azienda di Redmond – si basa sull'impegno alla trasparenza sulla raccolta, l'uso e la distribuzione dei dati.

La presenza dell'autenticazione multi-fattore (MFA), una funzione attivata dall'amministratore, protegge il nome utente e la password dell'utente, richiedendo una seconda forma di verifica per dimostrare la propria identità. Questo semplice processo di verifica a due fattori è oggi ampiamente utilizzato in molti settori, tra cui quello bancario, e protegge dalla maggior parte degli attacchi che sfruttano password deboli o rubate. Teams, cripta anche i dati in transito, memorizzando gli stessi nella propria rete sicura di data center e utilizzando il protocollo SRTP (Secure Real-time Transport Protocol) per la condivisione di video, audio e desktop.

Microsoft dichiara, inoltre, di rispettare le normative globali, nazionali, regionali e specifiche in materia di protezione dei dati personali, tra i quali spicca il GDPR.

Meet

La soluzione proposta dal gigante di Mountain View ha caratteristiche che coniugano sicurezza e privacy con la fruibilità.

Google afferma che, al pari delle altre sue soluzioni, l'utente conserva il controllo dei dati; dati che non vengono utilizzati per pubblicità né per vendita a terzi. In Meet – dichiara Google – i dati dei clienti sono criptati durante la trasmissione e le **registrazioni sono memorizzate in Google Drive** con criptazione di default. Meet non dispone di funzioni che monitorano l'attenzione dell'utente (una peculiarità di Zoom). Google dichiara che è possibile impostare policy di conservazione per le registrazioni usufruendo – in combinazione con Meet – di Google Vault.

Per quanto attiene la crittografia, Google dichiara che i dati trattati mediante Meet sono crittografati by-default in trasmissione tra il client e Google per le videochiamate su un browser web, sulle app Meet di Android e iOS e nelle "sale riunioni" con hardware dedicato.

Google specifica che se si partecipa a una riunione video per telefono, l'audio utilizza la rete dell'operatore telefonico e potrebbe non essere crittografato.

Anche le registrazioni delle riunioni memorizzate in Google Drive sono crittografate by-default. Meet, dichiara Google, aderisce agli standard di sicurezza della Internet Engineering Task Force (IETF) per la sicurezza dei livelli di trasporto Datagram Transport Layer Security (DTLS) e Secure Real-time Transport Protocol (SRTP).