Analisi dei Rischi e Valutazione di Impatto sulla Protezione dei dati relativamente ai trattamenti di dati effettuati con le piattaforme in cloud di Google e Microsoft	**Capital Security Srls** Via Montenapoleone, 8 20121 Milano Tel. 02-94750.267 info@capitalsecurity.it www.capitalsecurity.it

Google Workspace For Education

Microsoft Office 365

Titolo documento:	**Analisi dei Rischi e Valutazione di Impatto sulla Protezione dei dati**
Codice documento:	Risk Assessment & DPIA – Ver 1.0
Nome file:	Risk Assessment & DPIA – Ver 1.0
Stato documento:	Definitivo
Versione:	1.0
Data ultimo aggiornamento	23 marzo 2023

Capital Security Srls
Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Indice

Capital Security Srls
Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Art. 1 - Definizioni

Di seguito si riportano alcune definizioni rilevanti ai fini del presente regolamento; per le altre definizioni si rimanda all'art. 4 del Reg. UE 2016/679 – GDPR (per brevità nel seguito detto anche semplicemente "*Regolamento"* o "*GDPR*").

Ai sensi dell'art. 4 del Regolamento si intende per:

1) «dati personali»: qualsiasi informazione riguardante una persona fisica identificata o identificabile, (l'«interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, in particolare con riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici dell'identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale di tale persona fisica;

2) «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

3) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

4) «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti

Capital Security Srls
Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

5) «pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che i dati personali non siano attribuiti a una persona fisica identificata o identificabile;

6) «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

7) «autorità competente»:

a)qualsiasi autorità pubblica competente in materia di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica; o

b)qualsiasi altro organismo o entità incaricati dal diritto dello Stato membro di esercitare l'autorità pubblica e i poteri pubblici a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica;

8) «titolare del trattamento»: l'autorità competente che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o dello Stato membro, il titolare del trattamento o i criteri specifici applicabili alla sua nomina possono essere previsti dal diritto dell'Unione o dello Stato membro;

9) «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

Capital Security Srls
Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

10) «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o dello Stato membro non sono considerate destinatari; il trattamento di tali dati da parte di tali autorità pubbliche è conforme alle norme in materia di protezione dei dati applicabili secondo le finalità del trattamento;

11) «violazione dei dati personali»: la violazione della sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

12) «dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica, che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

13) «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

14) «dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

15) «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 41;

16) «organizzazione internazionale»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

Capital Security Srls
Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Art. 2 - Obiettivo del presente Regolamento

Sulla base del principio di accountability (responsabilizzazione) previsto dal Regolamento UE 2016/679 (GDPR), i titolari del trattamento sono tenuti a condurre un'analisi del rischio o valutazione d'impatto ed una verifica di adeguatezza circa le modalità, le garanzie ed i limiti del trattamento dei dati personali nel rispetto della normativa vigente in materia di sicurezza e protezione dei dati.

Scopo del presente documento è quindi quello di riassumere e formalizzare le risultanze principali dell'attività di analisi dei rischi condotta in conformità a quanto previsto dall'art. 32 del GDPR e della valutazione di impatto effettuata in conformità con quanto previsto dall'art. 35 del GDPR.

Art. 3 - Ambito di applicazione dell'Analisi dei Rischi e della Valutazione di Impatto sulla Protezione dei Dati

Le attività di analisi dei rischi e di valutazione di impatto sulla protezione dei dati sono state svolte con particolare riferimenti ai seguenti ambiti:

- trattamenti di dati personali e sensibili effettuate mediante piattaforme in cloud di Google, con particolare riferimento alla piattaforma Google Workspace for Education, e
- Microsoft Office 365.

Capital Security Srls
Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Art. 4 - Analisi dei Rischi

4.1 Rischi derivanti dalla perdita di riservatezza

Nella piattaforma Google tutti i prodotti sono protetti in modo continuo da una adeguata infrastruttura di sicurezza, completamente ridondata e fault-tolerant, cosicché è possibile resistere efficacemente a tutti i tentativi illeciti di accedere ai dati.

Il meccanismo di sicurezza integrata di Google rileva le minacce tramite sofisticati meccanismi e strumenti di Intrusion Detection ed interviene preventivamente per eliminare o contrastare le minacce ancora prima che queste possano causare danni o perdita di riservatezza delle informazioni.

Nei data center di Google i dati at-rest sono cifrati per impostazione predefinita.

I dati sono protetti con più livelli di sicurezza che includono tecnologie di crittografia all'avanguardia, come i protocolli HTTPS e Transport Layer Security. I data center di Google utilizzano un hardware personalizzato su cui sono in esecuzione un sistema operativo e un file system protetti personalizzati. Ciascuno di questi sistemi è stato ottimizzato per la sicurezza e le prestazioni.

Dal momento che Google controlla tutto l'hardware, è possibile di reagire rapidamente a qualsiasi minaccia o all'eventuale individuazione di punti deboli.

Inoltre tutti gli accessi alla piattaforma Google Workspace for Education sono protetti da credenziali di autenticazione che sono attribuite e gestite su base strettamente nominativa ed individuale.

Dal punto di vista della Scuola, è stato messo in atto un processo strutturato e tracciabile sulla base del quale gli account di soggetti che non hanno più titolo ad accedere alla piattaforma (ed. dimissioni, pensionamenti, trasferimenti, cambi di funzioni etc.) sono tempestivamente disabilitati senza venire cancellati. Le password

Capital Security Srls
Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

sono cifrate per cui anche se il traffico di rete venisse intercettato non sarebbe possibile decifrarle.

E' stato impostato un meccanismo che obbliga l'utente a modificare obbligatoriamente la propria password all'atto del primo utilizzo, al fine di ripristinarne la riservatezza.

E' inoltre possibile impedire il riutilizzo delle ultime n password, e forzare meccanismi di robustezza delle stesse.

Sulla base di tutto quanto sopra esposto, è possibile affermare che il rischio di perdita di riservatezza è estremamente basso.

Le stesse considerazioni possono essere fatte per le piattaforme in cloud di Microsoft.

4.2 Rischi derivanti dalla perdita di integrità

Poiché l'accesso ai dati avviene solamente a fronte di una procedura di autenticazione, e sulla base di un meccanismo di profilazione l'utente può accedere solo ed esclusivamente alle risorse (file, cartelle, stampanti etc.) alle quali è stato abilitato dall'amministratore di sistema, i rischi di perdita di integrità sono obiettivamente molto bassi.

Inoltre Google dispone di un meccanismo di logging (tracciatura) molto ricco e sofisticato, che permette di risalire a chi ha fatto che cosa, su quale oggetto, e quindi di individuare e gestire casistiche di eventuale compromissione dell'integrità.

Le stesse considerazioni possono essere fatte per le piattaforme in cloud di Microsoft.

4.3 Rischi derivanti dalla perdita di disponibilità

All'interno dei data center di Google vengono continuamente effettuate delle immagini totali (macchina + dati), che rappresentano di fatto una sorta di backup

Capital Security Srls
Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

continuo, che permette in caso di perdita o cancellazione accidentale dei dati di recuperare la versione precedente.

Inoltre Google possiede numerosi siti di disaster recovery, che vengono utilizzati in caso si verifichino eventi catastrofici come ad esempio incendi o inondazioni.

Le stesse considerazioni possono essere fatte per le piattaforme in cloud di Microsoft.

4.4 Rischi derivanti dalla mancata conformità al GDPR relativamente ai trasferimenti all'estero

La base giuridica che legittima il trasferimento di dati verso paesi terzi da parte di Google, Microsoft e migliaia di altre piattaforme in cloud (come ad esempio Facebook, Twitter, Instagram, Youtube, WeSchool, Canva, Activelylearn, Quizlet, Padlet, Scratch, Prezi etc.) è il combinato disposto dell'art. 46 comma 2 lettere c) e d) del GDPR con le Clausole Contrattuali Standard (SCC - Standard Contractual Clauses) approvate il 4 luglio 2021 dalla Commissione Europea.

Le stesse considerazioni possono essere fatte per le piattaforme in cloud di Microsoft.

Capital Security Srls
Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Art. 5 - Valutazione di Impatto sulla Protezione dei Dati

Sulla base dell'analisi dei rischi effettuata nei punti precedenti, la situazione riassuntiva può essere sintetizzata come segue:

Fattore di Rischio	Google	Microsoft
Rischi derivanti dalla perdita o compromissione della riservatezza	**BASSO**	**BASSO**
Rischi derivanti dalla perdita o compromissione dell'integrità	**BASSO**	**BASSO**
Rischi derivanti dalla perdita o compromissione della disponibilità	**BASSO**	**BASSO**
Rischi derivanti dalla mancata conformità al GDPR relativamente ai trasferimenti all'estero	**BASSO**	**BASSO**

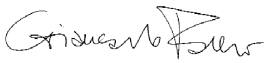
Art. 6 - Esito della Valutazione di Impatto sulla Protezione dei Dati

Sulla base delle considerazioni formalizzate nei punti precedenti, la valutazione di impatto è stata superata con esito positivo.

Capital Security Srls
Via Montenapoleone, 8
20121 Milano
Tel. 02-94750.267
info@capitalsecurity.it
www.capitalsecurity.it

Milano, 23/03/2023

Dott. Giancarlo Favero



Direttore
Capital Security Srls
Via Montenapoleone, 8
20121 Milano