Aspetti legali da considerare quando la PA acquisisce software

26 Giugno 2023

Avv. Marco Ciurcina
ciurcina@studiolegale.it

Di cosa parliamo

- GDPR (nozioni di base, obblighi, diritti, sentenze Schrems)
- CAD (valutazione comparativa)
- Statuto del Lavoratori (strumenti di controllo a distanza, 300/70)

Avv. Marco Ciurcina
ciurcina@studiolegale.it

e SaaS?

- Gsuite,
- Office365,
- Dropbox,
- Posta elettronica,
- WhatsApp,
- Google Analytics,
- Ecc.

Avv. Marco Ciurcina
ciurcina@studiolegale.it

GDPR: gli obblighi

per dati di persone fisiche

Tutela dei dati personali (GDPR)

Avv. Marco Ciurcina
ciurcina@studiolegale.it

GDPR: gli obblighi

A) Da fare:

- attuare in modo efficace i principi ex art. 5.1 GDPR
- soddisfare le condizioni di liceità ex art. 6.1 GDPR
- rispettare i vincoli ex artt. 9 e 10 GDPR
- fornire l'informativa agli interessati (artt. 13 e 14 GDPR)
- attuare i principi di privacy by design e by default (art. 25 GDPR)
- redigere accordi con i contitolari del trattamento e/o **contratti** o altri atti giuridici **con i responsabili del trattamento** (artt. 26 e **28 GDPR**)
- redigere le istruzioni agli incaricati del trattamento (art. 29 GDPR)
- tenere il registro delle attività di trattamento (art. 30 GDPR)
- garantire un livello di sicurezza adeguato al rischio (art. 32 GDPR)
- designare il responsabile della protezione dei dati personali (art. 37 GDPR)

Avv. Marco Ciurcina
ciurcina@studiolegale.it

GDPR: gli obblighi

B) Da valutare (e fare se necessario):

- eseguire la **valutazione d’impatto sulla protezione dei dati** (**art. 35 GDPR**)
- rispettare le condizioni di liceità del **trasferimento dei dati all’estero** (**artt. 44-50 GDPR**)
- redigere l’informativa e/o il banner cookie (art. 122 Codice Privacy)

Avv. Marco Ciurcina
ciurcina@studiolegale.it

GDPR: gli obblighi

C) Da monitorare nel tempo (e fare quando necessario):

- replicare alle richieste degli interessati ed inviare le notifiche (artt. 15-22 GDPR)
- eseguire la notifica al Garante della Privacy e la comunicazione all’interessato (artt. 33 e 34 GDPR)
- eseguire la consultazione preventiva ex art. 36 GDPR)
- aderire a codici di condotta e/o adottare certificazioni (artt. 40-43 GDPR)
- aggiornare le misure di cui ai punti A e B.

Avv. Marco Ciurcina
ciurcina@studiolegale.it

Di cosa parliamo

SaaS e GDPR

- DPA,
- DPIA,
- Trasferimento all’estero (e sentenze Schrems)

Avv. Marco Ciurcina
ciurcina@studiolegale.it

GDPR: gli obblighi

Art. 28 GDPR e SaaS

Tra gli obblighi, contrattualizzare responsabili del trattamento (inclusi i fornitori di SaaS che implicano il trattamento) ai sensi dell’art. 28 GDPR

Avv. Marco Ciurcina
ciurcina@studiolegale.it

GDPR: gli obblighi

Art. 35 GDPR

Valutazione d’impatto

sul trattamento dei dati personali

Il Garante: in vigenza dell'emergenza non era necessaria la valutazione di impatto, se il trattamento dei dati effettuato dalle istituzioni scolastiche, non presentava ulteriori caratteristiche suscettibili di aggravarne i rischi (ad esempio, era effettuato da una singola scuola, non, su larga scala, nell’ambito dell’utilizzo di un servizio on line di videoconferenza o di una piattaforma che non consentiva il monitoraggio sistematico degli utenti).

(conferma la recente circolare del Ministero dell’Istruzione e del Merito)

Avv. Marco Ciurcina
ciurcina@studiolegale.it

GDPR: gli obblighi

Art. 44-50 GDPR e SaaS

Condizioni di liceità del trasferimento extra UE

- Decisione di adeguatezza (art. 45 GDPR)
- Clausole contrattuali tipo (art. 46.2.c GDPR)
- Ecc.

Avv. Marco Ciurcina
ciurcina@studiolegale.it

GDPR: gli obblighi

Art. 45 GDPR e SaaS

2013: rivelazioni di Snowden, Risoluzione del Parlamento UE, Comunicazione della Commissione UE

2015: sentenza CGUE cd. Schrems I

2016: Privacy Shield

Avv. Marco Ciurcina
ciurcina@studiolegale.it

GDPR: gli obblighi

Art. 45 GDPR e SaaS

16/07/2020

Schrems II

Il Privacy Shield è nullo

Il diritto USA non offre adeguate garanzie di tutela dei diritti degli interessati: il fornitore statunitense è soggetto a norme (FISA 702 e E.O. 12333, in combinato disposto con PPD-28) che permettono attività di sorveglianza di massa in modo non rispettoso dei diritti fondamentali riconosciuti nell'UE

Avv. Marco Ciurcina
ciurcina@studiolegale.it

GDPR: gli obblighi

Art. 46.2.c GDPR e SaaS

Raccomandazioni 01/2020 relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE del 10 novembre 2020 (versione 2.0 del 18 giugno 2021)

https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en

Avv. Marco Ciurcina
ciurcina@studiolegale.it

GDPR: gli obblighi

Art. 46.2.c GDPR e SaaS

Raccomandazioni 1/2020 EDPB

Clausole Contrattuali Tipo, ma:

- eseguire la valutazione del diritto del paese nel quale si esegue il trasferimento (**TIA**);
- prevedere **idonee misure supplementari** (come per esempio la criptazione dei dati personali) di modo che non sia possibile utilizzare i dati personali in violazione dei diritti degli utenti al di fuori dell'UE.

Avv. Marco Ciurcina
ciurcina@studiolegale.it

GDPR: gli obblighi

CNIL

No approccio basato sul rischio

"*I titolari del trattamento possono adottare un approccio basato sul rischio, tenendo conto della probabilità di richieste di accesso ai dati?*

No…"

https://www.cnil.fr/en/qa-cnils-formal-notices-concerning-use-google-analytics

Avv. Marco Ciurcina
ciurcina@studiolegale.it

GDPR: gli obblighi

Art. 46.2.c GDPR e SaaS

Raccomandazioni 1/2020 EDPB

“Si osservi che anche l’accesso remoto da parte di un’entità di un paese terzo a dati situati nel SEE è considerato un trasferimento” (nota 22).

N.B.: il Clarifying Lawful Overseas Use of Data Act ("CLOUD Act"): consente alle autorità statunitensi di accedere ai dati contenuti nei server delle società statunitensi, anche se gestiti al di fuori degli Stati Uniti

Avv. Marco Ciurcina
ciurcina@studiolegale.it

GDPR: gli obblighi

EDPB

"2022 Azione esecutiva coordinata - Utilizzo di servizi basati su cloud da parte del settore pubblico" adottato come raccomandazione il 17 gennaio 2023:

"*..Emerge dall'analisi effettuata dalle Autorità che* ***il solo uso di un Cloud Service Provider che sia parte di un gruppo multinazionale soggetto alla normativa di paesi terzi, può risultare nell'applicazione di tale normativa anche a dati salvati nel EEA****. Eventuali richieste verrebbero inviate direttamente al CSP presente nel EEA e riguarderebbero dati presenti nel EEA e non dati già oggetto di trasferimenti..*"

Avv. Marco Ciurcina
ciurcina@studiolegale.it

GDPR: scenari

COSA CI RISERVA IL FUTURO?

Privacy Shield 2.0?

- 18.03.22: Biden e Von der Layen firmano una dichiarazione congiunta della Commissione europea e degli Stati Uniti sul quadro transatlantico sulla privacy dei dati;
- 7.10.22: Il Presidente Biden firma l'Executive Order "Enhancing Safeguards for United States Signals Intelligence Activities" (nuove tutele per la privacy e meccanismi di supervisione per l'intelligence straniera; può costituire la base di un nuovo quadro UE-USA sulla privacy?);
- 13.12.22: La Commissione avvia il processo di adozione della decisione di adeguatezza per la sicurezza dei flussi di dati con gli USA.

Avv. Marco Ciurcina
ciurcina@studiolegale.it

GDPR: scenari

COSA CI RISERVA IL FUTURO?

Privacy Shield 2.0?

- Comitato europeo per la protezione dei dati (EDPB) → Parere 5/2023
- Commissione LIBE del Parlamento Europeo → parere negativo della Commissione per le Libertà Civili, la Giustizia e gli Affari interni del Parlamento europeo (Commissione LIBE)

Avv. Marco Ciurcina
ciurcina@studiolegale.it

GDPR: scenari

COSA CI RISERVA IL FUTURO?

Privacy Shield 2.0?

Risoluzione del Parlamento europeo dell'11 maggio 2023

sull'adeguatezza della protezione offerta dal quadro UE-USA

in materia di privacy dei dati

https://www.europarl.europa.eu/doceo/document/TA-9-2023-0204_IT.html

Avv. Marco Ciurcina
ciurcina@studiolegale.it

GDPR: scenari

COSA CI RISERVA IL FUTURO?

Privacy Shield 2.0?

Risoluzione del Parlamento europeo dell'11 maggio 2023

"***Conclusioni***

15. ricorda che, nella sua risoluzione del 20 maggio 2021, il Parlamento ha invitato la Commissione a non adottare alcuna nuova decisione di adeguatezza in relazione agli Stati Uniti, a meno che non siano state introdotte riforme significative, in particolare a fini di sicurezza nazionale e intelligence; non ritiene che l'ordinanza esecutiva n. 14086 sia sufficientemente significativa; ribadisce che la Commissione non dovrebbe lasciare il compito di proteggere i diritti fondamentali dei cittadini dell'UE alla Corte di giustizia dell'Unione europea in conseguenza di denunce presentate dagli stessi singoli cittadini"

Avv. Marco Ciurcina
ciurcina@studiolegale.it

GDPR: scenari

COSA CI RISERVA IL FUTURO?

Privacy Shield 2.0?

Risoluzione del Parlamento europeo dell'11 maggio 2023

“***Conclusioni***

…

16. ricorda che la Commissione deve valutare l'adeguatezza di un paese terzo basandosi sulla legislazione e sulle pratiche in vigore, non solo nella sostanza ma anche nella pratica, come stabilito nelle sentenze Schrems I, Schrems II e nel RGPD (considerando 104)”

Avv. Marco Ciurcina
ciurcina@studiolegale.it

GDPR: scenari

COSA CI RISERVA IL FUTURO?

Privacy Shield 2.0?

Risoluzione del Parlamento europeo dell'11 maggio 2023

"***Conclusioni***

…

17. osserva che i principi del quadro in materia di privacy dei dati del Dipartimento del commercio degli Stati Uniti non hanno subito modifiche sufficienti, rispetto a quelle previste dallo scudo per la privacy, al fine di fornire una protezione sostanzialmente equivalente a quella prevista dal RGPD"

Avv. Marco Ciurcina
ciurcina@studiolegale.it

GDPR: scenari

COSA CI RISERVA IL FUTURO?

Privacy Shield 2.0?

Risoluzione del Parlamento europeo dell'11 maggio 2023

"***Conclusioni***

…

18. osserva che, mentre gli Stati Uniti stanno assumendo un impegno importante per migliorare l'accesso ai mezzi di ricorso e alle norme sul trattamento dei dati da parte delle autorità pubbliche, la comunità dell'intelligence statunitense ha tempo fino a ottobre 2023 per aggiornare le proprie politiche e pratiche in linea con l'impegno dell'ordinanza esecutiva n. 14086, e che l'Advocate General degli Stati Uniti non ha ancora definito l'UE e i suoi Stati membri come paesi che soddisfano i requisiti per poter accedere ai mezzi di ricorso disponibili dinanzi al Tribunale; sottolinea che ciò significa che la Commissione non è stata in grado di valutare "in pratica" l'efficacia dei mezzi di ricorso delle misure proposti in materia di accesso ai dati; conclude, pertanto, che la Commissione può solamente procedere con la fase successiva di una decisione di adeguatezza una volta che tali scadenze e obiettivi fondamentali siano soddisfatti dagli Stati Uniti per garantire che gli impegni siano rispettati nella pratica"

Avv. Marco Ciurcina
ciurcina@studiolegale.it

GDPR: scenari

COSA CI RISERVA IL FUTURO?

Privacy Shield 2.0?

Risoluzione del Parlamento europeo dell'11 maggio 2023

“***Conclusioni***

…

19. conclude che il quadro UE-USA in materia di privacy dei dati non crea un'equivalenza essenziale del livello di protezione; invita la Commissione a proseguire i negoziati con le sue controparti statunitensi al fine di creare un meccanismo che garantisca tale equivalenza, nonché l'adeguato livello di protezione richiesto dal diritto dell'Unione in materia di protezione dei dati e dalla Carta secondo l'interpretazione della CGUE; ***invita la Commissione a non adottare la decisione di adeguatezza fino a quando non saranno pienamente attuate tutte le raccomandazioni*** *formulate nella presente risoluzione e nel parere del comitato europeo per la protezione dei dati”*

Avv. Marco Ciurcina
ciurcina@studiolegale.it

GDPR: scenari

COSA CI RISERVA IL FUTURO?

Privacy Shield 2.0?

Risoluzione del Parlamento europeo dell'11 maggio 2023

"***Conclusioni***

…

20. invita la Commissione ad agire nell'interesse delle imprese e dei cittadini dell'UE garantendo che il quadro proposto fornisca una base giuridica solida, sufficiente e orientata al futuro per i trasferimenti di dati UE-USA; si attende che qualsiasi decisione di adeguatezza, se adottata, sia di nuovo impugnata dinanzi alla CGUE; ***sottolinea la responsabilità della Commissione nella mancata tutela dei diritti dei cittadini dell'UE nel caso in cui la decisione di adeguatezza sia nuovamente invalidata dalla CGUE***"

Avv. Marco Ciurcina
ciurcina@studiolegale.it

GDPR: scenari

COSA CI RISERVA IL FUTURO?

...intanto...

La multa a Meta Ireland di 1,2 Miliardi dall'EDPB

"A seguito della decisione vincolante di risoluzione delle controversie dell'EDPB del 13 aprile 2023, Meta Platforms Ireland Limited (Meta IE) ha ricevuto dall'Autorità irlandese per la protezione dei dati (IE DPA) una multa di 1,2 miliardi di euro a seguito di un'indagine sul suo servizio Facebook. Questa multa, che è la più grande mai comminata per il GDPR, è stata imposta per i trasferimenti di dati personali negli Stati Uniti da parte di Meta sulla base di clausole contrattuali standard (SCC) dal 16 luglio 2020. Inoltre, a Meta è stato ordinato di rendere i suoi trasferimenti di dati conformi al GDPR."

https://edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en

Avv. Marco Ciurcina
ciurcina@studiolegale.it

Acquisire software

C.A.D. - D. Lgs. 82/05 art. 68

Valutazione comparativa
e preferenza per il software libero

Art. 68 D. Lgs. 82/2005

Analisi comparativa delle soluzioni

1. Le pubbliche amministrazioni acquisiscono programmi informatici o parti di essi nel rispetto dei principi di economicità e di efficienza, tutela degli investimenti, riuso e neutralità tecnologica, a seguito di una valutazione comparativa di tipo tecnico ed economico tra le seguenti soluzioni disponibili sul mercato:

a) software sviluppato per conto della pubblica amministrazione;

b) riutilizzo di software o parti di esso sviluppati per conto della pubblica amministrazione;

c) software libero o a codice sorgente aperto;

d) software fruibile in modalità cloud computing;

e) software di tipo proprietario mediante ricorso a licenza d'uso;

f) software combinazione delle precedenti soluzioni.

Art. 68 D. Lgs. 82/2005

Analisi comparativa delle soluzioni

1-bis. A tal fine, le pubbliche amministrazioni prima di procedere all'acquisto, secondo le procedure di cui al codice di cui al decreto legislativo n. 50 del 2016, effettuano una valutazione comparativa delle diverse soluzioni disponibili sulla base dei seguenti criteri:

a) costo complessivo del programma o soluzione quale costo di acquisto, di implementazione, di mantenimento e supporto;

b) livello di utilizzo di formati di dati e di interfacce di tipo aperto nonché di standard in grado di assicurare l'interoperabilità e la cooperazione applicativa tra i diversi sistemi informatici della pubblica amministrazione;

c) garanzie del fornitore in materia di livelli di sicurezza, conformità alla normativa in materia di protezione dei dati personali, livelli di servizio tenuto conto della tipologia di software acquisito.

Art. 68 D. Lgs. 82/2005

Analisi comparativa delle soluzioni

*1-ter. Ove dalla valutazione comparativa di tipo tecnico ed economico, secondo i criteri di cui al comma 1-bis, risulti motivatamente l'**impossibilità** di accedere a soluzioni già disponibili all'interno della pubblica amministrazione, o a software liberi o a codici sorgente aperto, adeguati alle esigenze da soddisfare, è consentita l'acquisizione di programmi informatici di tipo proprietario mediante ricorso a licenza d'uso. La valutazione di cui al presente comma è effettuata secondo le modalità e i criteri definiti dall'AgID.*

Linee Guida

Linee Guida su acquisizione e riuso di software per le pubbliche amministrazioni

(pubblicate il 13.05.2019)

https://www.agid.gov.it/sites/default/files/repository_files/lg-acquisizione-e-riuso-software-per-pa-docs_pubblicata.pdf

(in GU 23.05.2019)

https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2019-05-23&atto.codiceRedazionale=19A03233

Art. 4 L. 300/1970

Art. 4.

(Impianti audiovisivi e altri strumenti di controllo)

1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo...

Avv. Marco Ciurcina
ciurcina@studiolegale.it

Art. 4 L. 300/1970

...accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali.

In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale.

Avv. Marco Ciurcina
ciurcina@studiolegale.it

Art. 8 L. 300/1970

Art. 8.

(Divieto di indagini sulle opinioni)

È fatto divieto al datore di lavoro, ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore.

Avv. Marco Ciurcina
ciurcina@studiolegale.it

Grazie

ciurcina@studiolegale.it