# Commissione Europea sotto esame. Il provvedimento correttivo del Garante europeo su Microsoft 365

04/04/2024

DIRITTO EUROPEO E DELLA CONCORRENZA, PRIVACY E CYBERSECURITY, PROSPETTIVE

Adriano Garofalo
Federico Aluigi

In data 11 marzo 2024, il Garante Europeo della Protezione dei Dati (GEPD)[1] ha emanato un provvedimento[2] nei confronti della Commissione europea nel quale ha individuato, riguardo l'utilizzo di Microsoft 365[3], diverse violazioni del Regolamento (UE) 1725/2018, "sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati", noto come "*GDPR for EUIs*" (da ora, il "Regolamento")[4].

L'indagine alla base, mirata a verificare il corretto recepimento delle Raccomandazioni pubblicate nel 2020 dal GEPD sull'uso da parte delle istituzioni dell'Unione dei prodotti e servizi Microsoft[5], era stata avviata nel maggio 2021 in seguito alla sentenza della Corte di Giustizia dell'Unione Europea (CGUE) c.d. *Schrems II*[6].

In breve, tale controversia riguardava la non conformità di una c.d. decisione di adeguatezza - un atto con il quale la Commissione europea classifica il livello di protezione dei dati personali da parte di un Paese terzo come avente le

[1] Il Garante europeo è un'autorità di sorveglianza indipendente che assicura il rispetto delle norme in materia di privacy da parte delle istituzioni e degli organi dell'Unione Europea.
[2] Provvedimento dell'11.03.2024 n. EDPS/2024/05, si veda il seguente LINK.
[3] Microsoft 365 è una suite di servizi e applicazioni cloud offerta da Microsoft che, tra gli altri, include strumenti come Office, Outlook, Teams e OneDrive.
[4] GU L 295/39 del 21.11.2018.
[5] *EDPS Public Paper on: Outcome of own-initiative investigation into EU institutions' use of Microsoft product and services*, si veda il seguente LINK.
[6] CGUE 16.07.2020, Causa C-311/18, *Facebook Ireland e Schrems*.

adeguate garanzie per attuare il trasferimento - adottata nei confronti degli Stati Uniti, che autorizzava il trasferimento nel paese di dati provenienti dallo Spazio Economico Europeo (SEE).

Tra le violazioni individuate dal GEPD, la Commissione europea, identificata come titolare del trattamento, ha mancato di adempiere all'obbligo, sulla base degli articoli 4 e 29 del Regolamento, di determinare con precisione quali dati possono essere trasferiti, per quali finalità e in quali Paesi terzi. Infatti, le c.d. istruzioni documentate sulla base delle quali Microsoft – identificata quale responsabile del trattamento – avrebbe dovuto attenersi ed essere sorvegliata dalla Commissione, non sono state considerate come sufficientemente chiare e precise dal GEPD.

Vi sono inoltre inadempienze riguardo gli articoli 4, 46 e 48 del Regolamento in proposito al trasferimento di dati personali in Paesi terzi al di fuori dello SEE che garantiscono un livello di protezione sostanzialmente equivalente a quello previsto dal Regolamento. Anche in questo caso, ciò sarebbe da imputare all'imprecisione ed alla povertà contenutistica evidenziate dal GEPD nel contratto siglato con Microsoft dalla Commissione.

È interessante notare come, prima dell'accordo USA-UE sul trasferimento di dati personali (*Data Privacy Framework EU-US*, entrato in vigore il 23 luglio 2023)[7], la Commissione abbia mancato di verificare se fosse necessario predisporre "misure di sicurezza supplementari", vale a dire specifiche misure tecniche, organizzative o contrattuali in grado di colmare il *gap* tra il livello di protezione richiesto dall'Unione e quello, più basso, garantito dal paese di destinazione del dato.

Nemmeno le Clausole Contrattuali Standard (CCS)[8] inserite dalla Commissione europea sono state ritenute sufficienti, poiché non chiare, non esaustive e non preventivamente sottoposte all'approvazione del GEPD così come richiesto dall'art. 48(3)(a) del Regolamento.

Allo stesso modo, gli accordi non sono trasparenti in merito ai sub-fornitori di Microsoft che potrebbero entrare in contatto con i dati personali e, pertanto, è stato rilevato come la Commissione non possa esercitare quel controllo che sarebbe previsto dal Regolamento, tra cui garantire un'adeguata protezione ai dati oppure assicurarsi che i medesimi siano esclusivamente trattati nei limiti delle sue istruzioni.

Tutto ciò considerato, il GEPD ha ordinato alla Commissione europea, a partire dal 9 dicembre 2024, di sospendere tutti i flussi di dati relativi all'utilizzo di Microsoft 365 verso Microsoft e le società affiliate che si trovano in Paesi al di fuori dello SEE nei confronti dei quali non si applica una decisione di adeguatezza.

Inoltre, entro la suddetta data, il trattamento dei dati derivanti dall'utilizzo di Microsoft 365 deve essere regolarizzato tramite, in primo luogo, una precisa mappatura che identifichi quali dati personali vengono trasferiti, verso quali Stati, quali sono le finalità del trattamento e quali sono le garanzie di protezione previste. Secondariamente, viene prescritto di garantire, mediante disposizioni contrattuali concluse ai sensi dell'articolo 29, paragrafo 3, del Regolamento e di altre misure organizzative e tecniche, che: *i)* tutti i dati personali siano raccolti per scopi espliciti e specificati; *ii)* le categorie di dati personali siano sufficientemente determinate rispetto agli scopi per cui

[7] Per ulteriori informazioni si veda il seguente LINK.
[8] Le Clausole Contrattuali Standard sono strumenti legali utilizzati, in assenza di una decisione di adeguatezza, per facilitare il trasferimento dei dati da un Paese SEE a un Paese terzo che non è considerato in linea con gli standard di protezione dei dati personali europei. In particolare, esse sono un set di regole contrattuali standardizzate che le organizzazioni possono incorporare nei loro contratti per garantire che i dati personali trasferiti all'estero siano conformi alla normativa europea in materia di protezione degli stessi.

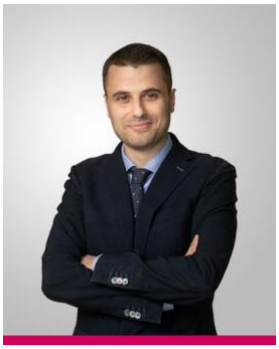
vengono trattati; *iii)* qualsiasi trattamento da parte di Microsoft, di sue controllate o di sub-fornitori sia effettuato solo in base alle istruzioni documentate della Commissione; *iv)* nessun dato personale sia ulteriormente trattato in modo non compatibile con gli scopi per cui è stato raccolto.

Il GEPD ha ordinato alla Commissione europea di dimostrare di aver adempiuto agli ordini di cui sopra entro il 9 dicembre 2024. Tale termine è stato individuato dal GEPD come risultato di un bilanciamento tra la gravità della violazione e la necessità di non compromettere il funzionamento dell'istituzione.

La vicenda in esame riporta *in auge* un tema già ampiamente dibattuto. L'Unione Europea, leader nell'implementare adeguate protezioni per la privacy dei cittadini, si trova spesso di fronte a contesti meno garantisti in altri Stati. In un panorama di rapida evoluzione politica ed economica, il controllo sui dati imposto dall'Unione si scontra talvolta con dinamiche socioeconomiche di altri paesi che non hanno implementato sistemi normativi così sofisticati, determinando un bilanciamento inadeguato tra la tutela della privacy e le altre esigenze in gioco.

Resta un tema aperto che potrebbe fornire ulteriori spunti, specialmente considerando che, nel luglio del 2023, l'avvocato e attivista Max Schrems ha indicato la possibilità di nuove questioni giuridiche da affrontare davanti alla Corte di Giustizia all'inizio dell'anno successivo. NOYB[9] ha già predisposto varie opzioni procedurali per contestare il *Data Privacy Framework EU-US*[10]*,* e l'organizzazione ha dimostrato di agire rapidamente: il caso Schrems II è stato presentato nel 2015, pochi mesi dopo la decisione di Schrems I e prima che il *Privacy Shield* UE-USA venisse formalmente adottato.

[9] Noyb è un'organizzazione senza scopo di lucro con sede a Vienna, fondata nel 2017. Guidata dall'avvocato austriaco e attivista per la privacy Max Schrems, essa mira ad instaurare casi giudiziari strategici e iniziative mediatiche a sostegno del GDPR.
[10] Per ulteriori informazioni, si veda il nostro precedente contributo al seguente LINK.




## Adriano Garofalo

**ASSOCIATE**

a.garofalo@dejalex.com
+39 02 72554.1
Via San Paolo 7
20121 - Milano



## Federico Aluigi

**ASSOCIATE**

f.aluigi@dejalex.com
+32 (0)26455670
Chaussée de La Hulpe 187
1170 - Bruxelles



MILANO
Via San Paolo, 7 · 20121 Milano, Italia
T. +39 02 72554.1 · F. +39 02 72554.400
milan@dejalex.com

ROMA
Via Vincenzo Bellini, 24 · 00198 Roma, Italia
T. +39 06 809154.1 · F. +39 06 809154.44
rome@dejalex.com

BRUXELLES
Chaussée de La Hulpe 187 · 1170 Bruxelles, Belgique
T. +32 (0)26455670 · F. +32 (0)27420138
brussels@dejalex.com

MOSCOW
Potapovsky Lane, 5, build. 2, 4th floor, office 401/12/9 · 101000, Moscow, Russia
T. +7 495 792 54 92 · F. +7 495 792 54 93
moscow@dejalex.com