

Bruxelles, 25 gennaio 2021
(OR. en)

5533/21

Fascicolo interistituzionale:
2020/0307(NLE)

SCH-EVAL 10
DATAPROTECT 13
COMIX 41

RISULTATI DEI LAVORI

Origine: Segretariato generale del Consiglio

Destinatario: Delegazioni

n. doc. prec.: 14247/20

Oggetto: Decisione di esecuzione del Consiglio recante raccomandazione relativa alla correzione delle carenze riscontrate nella valutazione 2019 dell'applicazione, da parte dell'**Ungheria**, dell'*acquis* di Schengen nel settore della **protezione dei dati**

Si allega per le delegazioni la decisione di esecuzione del Consiglio recante raccomandazione relativa alla correzione delle carenze riscontrate nella valutazione 2019 dell'applicazione, da parte dell'Ungheria, dell'*acquis* di Schengen nel settore della protezione dei dati, adottata mediante procedura scritta il 21 gennaio 2021.

In linea con l'articolo 15, paragrafo 3, del regolamento (UE) n. 1053/2013 del Consiglio, del 7 ottobre 2013, la presente raccomandazione sarà trasmessa al Parlamento europeo e ai parlamenti nazionali.

RACCOMANDAZIONE

relativa alla correzione delle carenze riscontrate nella valutazione 2019 dell'applicazione, da parte dell'Ungheria, dell'*acquis* di Schengen nel settore della protezione dei dati

IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il regolamento (UE) n. 1053/2013 del Consiglio, del 7 ottobre 2013, che istituisce un meccanismo di valutazione e di controllo per verificare l'applicazione dell'*acquis* di Schengen e che abroga la decisione del comitato esecutivo del 16 settembre 1998 che istituisce una Commissione permanente di valutazione e di applicazione di Schengen¹, in particolare l'articolo 15,

vista la proposta della Commissione europea,

considerando quanto segue:

- (1) Scopo della presente decisione è raccomandare all'Ungheria provvedimenti correttivi tesi a colmare le carenze riscontrate durante la valutazione Schengen nel settore della protezione dei dati eseguita nel 2019. A seguito della valutazione, con decisione di esecuzione C(2020) 8170 della Commissione è stata adottata una relazione riguardante i risultati e le valutazioni, che elenca le migliori pratiche e le carenze riscontrate.

¹ GU L 295 del 6.11.2013, pag. 27.

- (2) Tra le buone pratiche si osserva, tra l'altro, che il bilancio dell'Autorità nazionale per la protezione dei dati e per la libertà dell'informazione (in appresso NAIH) ha registrato un incremento costante, che l'ufficio SIRENE si è conformato alle raccomandazioni formulate nella precedente valutazione Schengen del 2012 nel settore della protezione dei dati e ora indica che gli interessati possono presentare un reclamo alla NAIH; che il ministero degli Affari esteri e del commercio (MFAT) indica anche la possibilità del ricorso giurisdizionale; che le informazioni fornite sul sito Internet della NAIH sono complete, utili e disponibili, facilmente accessibili e formulate con un linguaggio chiaro; che il MFAT si è adoperato per gestire e formalizzare i diversi aspetti della sicurezza delle informazioni; che il MFAT dispone di un piano solido e completo in materia di sicurezza e che i modelli per l'esercizio dei diritti degli interessati attinenti al Sistema di informazione Schengen (SIS II) sono disponibili in diverse lingue (ungherese, inglese, tedesco, francese e russo).
- (3) Non dovrebbe quindi essere data alcuna indicazione di priorità nell'attuazione delle raccomandazioni.
- (4) È opportuno trasmettere la presente decisione al Parlamento europeo e ai parlamenti degli Stati membri. Entro sei mesi dalla sua adozione, l'Ungheria deve, a norma dell'articolo 16, paragrafo 8, del regolamento (UE) n. 1053/2013, presentare alla Commissione una valutazione degli (eventuali) miglioramenti e una descrizione delle azioni richieste,

RACCOMANDA:

l'Ungheria è invitata a

Autorità per la protezione dei dati (NAIH)

1. provvedere a che la NAIH, nel verificare la conformità con la normativa relativa al SIS II, effettui anche ispezioni periodiche delle segnalazioni SIS II;
2. assicurare che la NAIH dia seguito alle conclusioni e alle raccomandazioni risultanti dalle ispezioni del SIS II e dagli audit delle precedenti misure di controllo e che se ne tenga conto anche nei piani di ispezione del 2019;
3. assicurare che la NAIH dia seguito in modo completo all'attuazione effettiva delle raccomandazioni formulate a seguito delle attività di controllo del Sistema di informazione visti (VIS);

4. assicurare che l'attività di controllo del sistema nazionale VIS da parte della NAIH copra tutti gli aspetti relativi alla protezione dei dati del sistema nazionale dei visti, compreso il trattamento da parte dei fornitori esterni di servizi;

Diritti degli interessati

5. ampliare l'ambito di applicazione dell'allegato 9 del decreto governativo 15/2013 (che istituisce un modello specifico per l'esercizio dei diritti di accesso degli interessati) al fine di introdurre anche modelli per l'esercizio degli altri diritti degli interessati, quali la rettifica e la cancellazione;
6. provvedere a che le autorità ungheresi (Direzione generale nazionale della polizia degli stranieri — OIF) chiariscano le loro procedure relative alla valutazione delle richieste degli interessati, in particolare quando esse limitano i diritti di rettifica o cancellazione, e le allineino al diritto dell'Unione e al diritto nazionale applicabile;

Sistema di informazione visti

7. assicurare che gli utilizzatori privilegiati del VIS siano adeguatamente monitorati; a tal fine può essere necessario adottare misure organizzative e tecniche;
8. aumentare la frequenza dei test relativi alla gestione della continuità operativa (BCM) e al piano di ripristino in caso di disastro (DRP), in particolare per il MFAT;
9. assicurare che, fino all'attuazione del sito IT secondario, nel breve termine tutto il backup dei sistemi informatici non sia conservato nello stesso locale che ospita i server, bensì al di fuori;
10. rafforzare la sicurezza di accesso al rack;
11. eseguire periodicamente un riesame della sicurezza del sistema di cifratura sviluppato a livello interno (MFAT);

Sistema di informazione Schengen

12. rafforzare la sicurezza fisica dell'edificio che ospita il centro dati dotando anche la seconda uscita/entrata di videosorveglianza e migliorare la sicurezza fisica dei rack nella sala server;
13. effettuare verifiche periodiche della sicurezza del sistema di gestione dell'accesso degli utilizzatori del SIS II;

14. provvedere a che sia applicato un corpus generale uniforme di direttive/linee guida relative alla sicurezza dell'informazione per l'N.SIS (ad esempio, politica in materia di password, ecc.);
15. assicurare che l'ufficio SIRENE, in collaborazione con l'archivio nazionale, valuti le possibilità di adottare una procedura di selezione più frequente per quanto riguarda la procedura di conservazione dei dati;
16. aumentare la frequenza dei test relativi alla gestione della continuità operativa (BCM) e al piano di ripristino in caso di disastro (DRP);
17. fare in modo che l'Ufficio nazionale di polizia ungherese (ORFK), e in particolare l'ufficio N.SIS e l'ufficio SIRENE, installino una soluzione informatica per monitorare gli utilizzatori privilegiati;
18. assicurare che l'ufficio SIRENE svolga un ruolo più attivo nel coordinamento della verifica della qualità delle informazioni inserite nel SIS II di cui all'articolo 1.15 del manuale SIRENE;

Sensibilizzazione del pubblico

19. assicurare che il MFAT definisca chiaramente il titolare o i titolari del trattamento ai fini del VIS. Per garantire la trasparenza e consentire alle persone di esercitare i loro diritti, è importante che gli interessati siano adeguatamente informati delle responsabilità di ciascun titolare del trattamento dei dati;
20. fare in modo che l'ORFK aggiorni regolarmente la versione inglese contenente la sezione sul SIS.

Fatto a Bruxelles, il

Per il Consiglio

Il presidente