Consiglio dell'Unione europea

Bruxelles, 24 settembre 2019
(OR. en)

12468/19

Fascicolo interistituzionale: 2019/0168(NLE)

SCH-EVAL 157
DATAPROTECT 216
COMIX 427

RISULTATI DEI LAVORI

Origine:	Segretariato generale del Consiglio
in data:	20 settembre 2019
Destinatario:	delegazioni
n. doc. prec.:	11904/19
Oggetto:	Decisione di esecuzione del Consiglio recante raccomandazione relativa alla correzione delle carenze riscontrate nella valutazione 2018 dell'applicazione, da parte della **Lituania**, 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 2018 dell'applicazione, da parte della Lituania, dell'*acquis* di Schengen nel settore della protezione dei dati, adottata dal Consiglio nella sessione del 20 settembre 2019.

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.

Decisione di esecuzione del Consiglio recante

RACCOMANDAZIONE

relativa alla correzione delle carenze riscontrate nella valutazione 2018 dell'applicazione, da parte della Lituania, 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 Schengen[1], in particolare l'articolo 15,

vista la proposta della Commissione europea,

considerando quanto segue:

(1) Scopo della presente decisione è raccomandare alla Lituania provvedimenti correttivi tesi a colmare le carenze riscontrate durante la valutazione Schengen nel settore della protezione dei dati eseguita nel 2018. A seguito della valutazione, con decisione di esecuzione C(2019) 5700 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 figurano: la consulenza e gli orientamenti forniti ai richiedenti dall'autorità per la protezione dei dati, che non si limita a inoltrare le richieste; la fornitura di lettere tipo per l'esercizio dei diritti degli interessati nell'ambito del sistema d'informazione Schengen II (SIS II) e del sistema di informazione visti (VIS); il livello generalmente elevato delle misure di sicurezza attuate presso i locali del dipartimento per la tecnologia dell'informazione e della comunicazione del ministero dell'Interno (che ospita l'N.VIS e l'N.SIS), che garantiscono un ambiente sicuro per la conservazione dei dati e la prevenzione degli incidenti; la formazione ben sviluppata per gli utenti finali del VIS, in particolare per il personale consolare prima del distacco presso le ambasciate/i consolati; l'impegno alla formazione e allo sviluppo del personale, in particolare una formazione ben sviluppata che copre anche la protezione dei dati per gli utenti finali dell'N.SIS e il personale dell'ufficio SIRENE; la completezza, l'utilità e la facilità di consultazione linguistica (disponibilità in diverse lingue) delle informazioni sul SIS II e sul VIS fornite dall'autorità per la protezione dei dati sul suo sito web; l'ottima qualità e l'accessibilità delle informazioni sul trattamento dei dati in entrambe le banche dati e sui relativi diritti degli interessati figuranti negli opuscoli dell'autorità per la protezione dei dati relativi alla protezione dei dati personali nel sistema d'informazione Schengen e alla protezione dei dati personali nel sistema d'informazione visti; il forte coinvolgimento dell'autorità per la protezione dei dati in molte conferenze, formazioni e altri eventi di sensibilizzazione, destinati anche al personale preposto al trattamento dei dati SIS II e VIS.

(3) Alla luce dell'importanza del rispetto dell'*acquis* di Schengen in materia di protezione dei dati, in particolare al fine di garantire la piena indipendenza dell'autorità per la protezione dei dati, è opportuno dare priorità all'attuazione della raccomandazione 1.

(4) È opportuno trasmettere la presente decisione al Parlamento europeo e ai parlamenti degli Stati membri. Entro tre mesi dalla sua adozione, la Lituania deve, a norma dell'articolo 16, paragrafo 1, del regolamento (UE) n. 1053/2013, elaborare un piano d'azione che elenchi tutte le raccomandazioni volte a correggere le carenze riscontrate nella relazione di valutazione e presentarlo alla Commissione e al Consiglio,

RACCOMANDA:

la Lituania è invitata a

Autorità di controllo per la protezione dei dati

1. al fine di garantire meglio la piena indipendenza dell'ispettorato nazionale per la protezione dei dati ("autorità per la protezione dei dati"), abolire i requisiti della previa approvazione del piano d'azione strategico dell'autorità per la protezione dei dati da parte del ministro della Giustizia e della previa consultazione del ministro della Giustizia in merito al piano d'azione annuale prima che il direttore dell'autorità per la protezione dei dati possa approvarlo. Tale aspetto è importante anche per garantire che la procedura di bilancio non presenti alcun elemento di rischio di violazione dell'indipendenza dell'autorità per la protezione dei dati;

2. al fine di garantire meglio la piena indipendenza dell'autorità per la protezione dei dati, organizzare le riunioni periodiche bilaterali tra il ministro della Giustizia e il direttore dell'autorità per la protezione dei dati in modo tale che queste riunioni non comportino un rischio di influenza diretta o indiretta del governo sull'autorità per la protezione dei dati, che potrebbe compromettere l'indipendenza di tale autorità;

3. abolire tutti quegli elementi di responsabilità del direttore dell'autorità per la protezione dei dati nei confronti del governo e del ministro della Giustizia che potrebbero comportare un rischio di influenza diretta o indiretta da parte del governo e del ministro della Giustizia e compromettere l'indipendenza dell'autorità per la protezione dei dati;

4. garantire che l'autorità per la protezione dei dati controlli con maggior frequenza la liceità del trattamento dei dati personali SIS II;

5. garantire che, almeno ogni quattro anni, l'autorità per la protezione dei dati effettui un audit dei trattamenti dei dati nell'N.SIS;

6. garantire che l'autorità per la protezione dei dati controlli la liceità del trattamento dei dati personali VIS. L'autorità per la protezione dei dati dovrebbe inoltre - quando effettua ispezioni presso le ambasciate - effettuare ispezioni dei trattamenti dei dati e della sicurezza dei dati presso i fornitori esterni di servizi; tale possibilità dovrebbe essere specificata nel contratto tra il ministero degli Affari esteri e i fornitori esterni di servizi;

7. garantire che, almeno ogni quattro anni, l'autorità per la protezione dei dati effettui un audit dei trattamenti dei dati nell'N.VIS;

Diritti degli interessati

8. garantire che il termine di 60 giorni per rispondere alle richieste degli interessati del SIS II di cui all'articolo 41, paragrafo 6, del regolamento SIS II e all'articolo 58, paragrafo 6, della decisione SIS II sia rispettato fino a quando diverrà pienamente applicabile (al più tardi il 28 dicembre 2021) il nuovo *acquis* del SIS[2], che contiene riferimenti incrociati ai termini di risposta alle richieste degli interessati di cui al regolamento generale sulla protezione dei dati[3] (30 giorni con possibilità di proroga di altri due mesi se necessario);

9. chiarire le procedure interne relative alla responsabilità delle autorità coinvolte per quanto riguarda i diritti degli interessati nell'ambito del SIS II. In tal modo il personale potrebbe inoltre essere a conoscenza delle persone a cui inoltrare le richieste;

---

[2] Regolamento (UE) 2018/1862 del Parlamento europeo e del Consiglio, del 28 novembre 2018, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale, che modifica e abroga la decisione 2007/533/GAI del Consiglio e che abroga il regolamento (CE) n. 1986/2006 del Parlamento europeo e del Consiglio e la decisione 2010/261/UE della Commissione (GU L 312 del 7.12.2018, pag. 56) (si vedano in particolare gli articoli da 66 a 71). Regolamento (UE) 2018/1861 del Parlamento europeo e del Consiglio, del 28 novembre 2018, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore delle verifiche di frontiera, che modifica la convenzione di applicazione dell'accordo di Schengen e abroga il regolamento (CE) n. 1987/2006 (GU L 312 del 7.12.2018, pag. 14) (si vedano in particolare gli articoli da 51 a 57).

[3] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

10. garantire che le risposte finali del ministero dell'Interno alle persone che intendono esercitare i diritti degli interessati nell'ambito del SIS II siano coerenti, in modo che siano fornite informazioni sul diritto di contestare la decisione dinanzi all'autorità per la protezione dei dati e sul diritto di proporre ricorso dinanzi agli organi giurisdizionali;

11. chiarire le procedure interne relative alla responsabilità delle autorità coinvolte per quanto riguarda i diritti degli interessati nell'ambito del VIS. In tal modo il personale potrebbe inoltre essere a conoscenza delle persone a cui inoltrare le richieste;

12. garantire che le risposte finali del ministero dell'Interno alle persone che intendono esercitare i diritti degli interessati nell'ambito del VIS siano coerenti, in modo che siano fornite informazioni sul diritto di contestare la decisione dinanzi all'autorità per la protezione dei dati e sul diritto di proporre ricorso dinanzi agli organi giurisdizionali;

Sistema d'informazione visti

13. adottare le misure necessarie per garantire che i contratti tra il ministero degli Affari esteri e i fornitori esterni di servizi disciplinino le modalità di coinvolgimento dell'autorità per la protezione dei dati lituana nelle ispezioni condotte dalle ambasciate/dai consolati e dal ministero degli Affari esteri;

14. migliorare l'autocontrollo verificando proattivamente e sistematicamente i registri al fine di monitorare la liceità del trattamento dei dati personali VIS. Il ministero dell'Interno dovrebbe sviluppare ulteriormente il sistema SIEM per il controllo automatico dei registri;

15. garantire che il responsabile della protezione dei dati del ministero degli Affari esteri sia maggiormente coinvolto nello sviluppo e nella fornitura di formazione sulla protezione dei dati destinata al personale del ministero degli Affari esteri, compresi i membri distaccati presso le ambasciate/i consolati;

Sistema di informazione Schengen II

16. eliminare la possibilità che un utente finale possa accedere, attraverso il browser POLIS, all'N.SIS con più dispositivi contemporaneamente;

17. garantire l'introduzione di carte intelligenti per l'accesso alle postazioni di lavoro degli utenti N.SIS all'interno della polizia al fine di migliorare il livello e le norme di sicurezza;

18. assicurare che le misure tecniche adottate per impedire l'uso di chiavi USB nelle postazioni di lavoro degli uffici SIRENE siano pienamente applicate e controllate periodicamente;

19. migliorare l'autocontrollo verificando proattivamente e sistematicamente i registri degli utenti finali SIS II di tutte le autorità interessate al fine di monitorare la liceità del trattamento dei dati personali SIS II; il ministero dell'Interno dovrebbe sviluppare ulteriormente il sistema SIEM per il controllo automatico dei registri;

20. assicurarsi che la conoscenza del personale per quanto riguarda la protezione dei dati in relazione alla gestione dei dati SIS II e VIS sia rafforzata attraverso regolari sessioni di aggiornamento;

21. garantire che la formazione e la sensibilizzazione del personale che ha accesso all'N.SIS siano un ambito guidato dal gruppo di responsabili della protezione dei dati del ministero dell'Interno. Ciò consentirà di garantire una struttura e una pianificazione continue per lo sviluppo del personale;

Sensibilizzazione del pubblico

22. garantire che i link sul sito web dell'autorità per la protezione dei dati relativi al SIS II e al VIS siano aggiornati periodicamente;

23. garantire che i siti web delle organizzazioni che hanno contatti con cittadini di altri paesi, quali il ministero dell'Interno, la polizia, la guardia di frontiera, il ministero degli Affari esteri e gli uffici consolari, forniscano informazioni accessibili e chiare sul SIS II, sul VIS e sui relativi diritti degli interessati anche in inglese;

24. garantire che quando i siti web forniscono informazioni sul SIS II, sul VIS e sui relativi diritti degli interessati in inglese, tali informazioni siano più facili da trovare;

25. garantire la coerenza delle informazioni sull'esercizio dei diritti degli interessati in relazione all'N.SIS II e al VIS figuranti sui siti web delle istituzioni che lavorano con tali sistemi;

26. aggiungere informazioni in merito al trattamento dei dati e ai relativi diritti degli interessati sul portale EPM attraverso cui i richiedenti forniscono dati ai fini delle domande di visto.

Fatto a Bruxelles, il

Per il Consiglio
Il presidente