Consiglio dell'Unione europea

Bruxelles, 25 gennaio 2021
(OR. en)

5534/21

Fascicolo interistituzionale: 2020/0304(NLE)

SCH-EVAL 11
DATAPROTECT 14
COMIX 42

RISULTATI DEI LAVORI

Origine:	Segretariato generale del Consiglio
Destinatario:	Delegazioni
n. doc. prec.:	14250/20
Oggetto:	Decisione di esecuzione del Consiglio recante raccomandazione relativa alla correzione delle carenze riscontrate nella valutazione 2019 della **Repubblica slovacca** sull'applicazione 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 della Repubblica slovacca sull'applicazione 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.

Decisione di esecuzione del Consiglio recante

RACCOMANDAZIONE

relativa alla correzione delle carenze riscontrate nella valutazione 2019 della Repubblica slovacca sull'applicazione 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 Repubblica slovacca provvedimenti correttivi per colmare le carenze riscontrate durante la valutazione Schengen 2019 nel settore della protezione dei dati. A seguito della valutazione, con decisione di esecuzione C(2020)8160 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, dall'ultima valutazione Schengen del 2012, l'autorità per la protezione dei dati (DPA) ha svolto regolarmente attività di controllo del SIS II sulla base di una pianificazione annuale, e che è stato elaborato un programma di ispezioni del SIS II per i prossimi quattro anni; che la DPA ha effettuato un numero considerevole di ispezioni VIS presso i consolati; che la DPA e il ministero dell'Interno si stanno adoperando per fornire informazioni agli interessati attraverso materiale cartaceo ed elettronico; che la DPA mette a disposizione versioni multilingue delle informazioni sui temi connessi a Schengen nel suo sito web e tramite opuscoli; che la DPA predispone dei modelli per le richieste di informazioni relative al SIS e al VIS; che l'ufficio SIRENE fornisce risposte non soltanto in lingua slovacca ma anche in inglese; che le autorità slovacche informano gli interessati qualora il SIS II non contenga dati che li concernono; che la sezione "Ispezioni" dell'Ufficio ispettivo del ministero dell'Interno effettua un controllo molto attivo dei registri del VIS e del SIS II; che i due membri del personale del Dipartimento per la sicurezza del ministero degli Affari esteri ed europei che si occupano di questioni relative alla protezione dei dati svolgono un ruolo molto attivo; che il ministero degli Affari esteri ed europei offre al proprio personale una formazione in materia di protezione dei dati, in particolare prima del distacco temporaneo presso i consolati, e che è il Dipartimento di sicurezza (nel suo ruolo di ufficio della protezione dei dati) a impartire tale formazione; che la sicurezza procedurale e fisica istituita per proteggere i dati SIS II è di elevato livello; che il responsabile della protezione dei dati e il suo vice nel Dipartimento per la protezione dei dati della sezione "Ispezioni" dell'Ufficio ispettivo del ministero dell'Interno svolgono un ruolo molto attivo, anche per quanto riguarda le linee guida e il controllo dei registri relativi al SIS II; che il ministero dell'Interno organizza attività di formazione in materia di protezione dei dati per tutti gli utilizzatori finali dell'N.SIS II.

(3) In considerazione dell'importanza del rispetto dell'*acquis* di Schengen nel settore della protezione dei dati in relazione al VIS, dovrebbe essere data priorità all'attuazione delle raccomandazioni 7 e 24.

(4) È opportuno trasmettere la presente decisione al Parlamento europeo e ai parlamenti degli Stati membri. Entro tre mesi dalla sua adozione, la Repubblica slovacca 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 Repubblica slovacca è invitata a:

Autorità per la protezione dei dati

1. provvedere a che siano ulteriormente incrementati il bilancio e il personale della DPA, al fine di rafforzarne le prestazioni e l'efficacia;

2. assicurare che la parte del bilancio generale attribuita dallo Stato alla DPA sia chiaramente visibile, al fine di garantire che la DPA disponga di un bilancio annuale pubblico e distinto;

3. provvedere a che, nella procedura di bilancio, il Consiglio nazionale sia informato della posizione della DPA sul proprio fabbisogno di bilancio e delle discussioni che si svolgono tra la DPA e il ministero delle Finanze sul bilancio;

4. adottare misure affinché il ministero delle Finanze non possa effettuare alcuna correlazione tra il bilancio e l'importo delle ammende che devono essere riscosse dalla DPA, in quanto ciò potrebbe ripercuotersi sulla natura e sulla definizione delle priorità di lavoro della DPA, compromettendone in tal modo l'indipendenza. Dovrebbe essere garantito che il bilancio della DPA non possa essere ridotto nel corso dell'anno civile in una situazione in cui le sanzioni previste non siano state interamente riscosse dalla DPA;

5. assicurare che alla DPA siano conferite tutte le mansioni e tutte le competenze previste per le autorità per la protezione dei dati negli articoli 57 e 58 del regolamento generale sulla protezione dei dati;

6. assicurare che in aggiunta alle regolari attività di controllo effettuate dall'ufficio N.SIS e dall'ufficio SIRENE, la DPA vigili sulle altre autorità che hanno accesso al SIS II e di cui sono utilizzatori finali;

7. provvedere a che le attività di controllo della DPA in relazione al VIS comprendano l'ispezione dell'autorità centrale per i visti (CVA) per quanto riguarda le operazioni di trattamento dei dati nell'N.VIS. Poiché il termine per il primo audit del sistema nazionale visti era il mese di ottobre 2015, la DPA dovrebbe eseguire quanto prima la parte ancora mancante dell'audit;

8. assicurare che la DPA effettui periodicamente ispezioni anche nei confronti dei fornitori esterni di servizi;

Diritti degli interessati

9. trovare un modo appropriato che permetta alla DPA, al ministero dell'Interno e al ministero degli Affari esteri ed europei di informare gli interessati in merito ai potenziali rischi legati alla trasmissione di copie delle carte d'identità e di informazioni sensibili attraverso canali non sicuri di Internet. Il ministero dell'Interno e il ministero degli Affari esteri ed europei sono invitati a prendere in considerazione la possibilità di offrire agli interessati un canale protetto per la trasmissione elettronica di tali documenti;

10. provvedere a 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 sarà pienamente applicabile (al più tardi il 28 dicembre 2021) il nuovo *acquis* relativo al SIS[1], nel quale vi sono riferimenti incrociati al termine per rispondere alle richieste degli interessati previsto nel RGPD (30 giorni con possibilità di proroga di altri due mesi se necessario);

11. considerare di fornire alcune delle informazioni stampate (opuscoli/cartelli ecc.) agli interessati nei locali delle stazioni di polizia e di renderle visibili e facilmente disponibili;

12. esaminare la possibilità di predisporre, ad esempio, una versione inglese informale delle decisioni della DPA sulle denunce riguardanti le richieste degli interessati del SIS II; ciò aiuterebbe gli interessati a comprendere meglio la decisione e rafforzerebbe così i loro diritti;

13. assicurare che le informazioni sui diritti degli interessati in relazione al VIS contenute nel sito web del ministero degli Affari esteri ed europei siano più facili da trovare; il sito web dovrebbe inoltre fornire modelli per l'esercizio dei diritti degli interessati in relazione al VIS;

---

[1] 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.

14. assicurare che il modulo per la domanda di visto contenga informazioni chiare sulle diverse autorità che trattano i dati personali nell'ambito del sistema nazionale dei visti. In particolare, dovrebbero essere fornite informazioni indicanti che il ministero degli Affari esteri ed europei è il titolare del trattamento dei dati;

15. fornire informazioni su supporto fisico (opuscoli/cartelli ecc.) agli interessati in relazione al VIS nei locali degli aeroporti e di altri punti in cui sono eseguiti controlli di frontiera e renderle visibili e facilmente accessibili;

16. provvedere a che le risposte agli interessati in merito ai dati personali del VIS forniscano informazioni sulla possibilità di impugnare la risposta dinanzi alla DPA e al tribunale competente;

17. adottare le misure necessarie per precisare le responsabilità del ministero degli Affari esteri ed europei e del CVA (ministero dell'Interno) per quanto riguarda il trattamento delle richieste degli interessati del VIS e per fornire linee guida interne o metodologiche a entrambi i ministeri; tali informazioni dovrebbero essere disponibili agli interessati;

Sistema di informazione visti

18. adottare le misure necessarie per aumentare il livello di sicurezza dell'accesso all'ambiente governativo e in particolare alle domande di visto nazionali presso il ministero degli Affari esteri ed europei e il CVA (ministero dell'Interno), in particolare mediante l'accesso alle banche dati nazionali dei visti attraverso la tecnologia di autenticazione multifattoriale;

19. adottare le misure necessarie per migliorare la sicurezza fisica e organizzativa nel centro dati N.VIS del ministero degli Affari esteri ed europei, in particolare per quanto riguarda i seguenti aspetti:

    – messa a disposizione di un registro dei visitatori all'ingresso del centro dati per il personale addetto alle TIC, i visitatori o i fornitori il cui accesso dovrebbe essere limitato;
    – installazione di un sistema di estinzione degli incendi mediante gas (aragonite);
    – installazione del rilevamento delle perdite d'acqua;
    – pulizia dei pavimenti, che devono essere ordinati e spolverati;
    – chiusura a chiave dei dispositivi di protezione dei server dell'UE;

20. accelerare la procedura per la creazione di un nuovo centro dati N.VIS in un'altra sede e il reinsediamento del centro dati;

21. considerare di modificare il periodo di conservazione locale dei file di registro N.VIS presso le missioni diplomatiche e consolari, stabilendolo in funzione di un periodo di tempo anziché della quantità di MB;

22. prendere in considerazione l'utilizzo di sistemi di controllo automatico dei registri presso il ministero degli Affari esteri ed europei;

23. prendere le misure necessarie affinché le missioni diplomatiche o il ministero degli Affari esteri ed europei effettuino periodiche ispezioni presso i fornitori esterni di servizi;

24. adottare le misure necessarie per assicurare una formazione più sistematica e uniforme in materia di protezione dei dati al personale consolare locale;

25. assicurare che la domanda di visto elettronico richieda le stesse informazioni del modulo cartaceo per la domanda di visto (come stabilito nell'allegato I del codice dei visti dell'UE[1]);

Sistema di informazione Schengen II

26. adottare le misure necessarie per migliorare il livello di sicurezza di accesso all'N.SIS II, in particolare utilizzando la tecnologia di autenticazione multifattoriale e unicamente i collegamenti https per l'accesso all'N.SIS II;

27. provvedere a che il ministero dell'Interno informi l'autorità di gestione dei dati di eventuali violazioni dei dati che potrebbero comportare un rischio per i diritti e le libertà delle persone fisiche. Inoltre, il ministero dell'Interno dovrebbe istituire un registro delle violazioni dei dati personali;

---

1 Regolamento (CE) n. 810/2009 del Parlamento europeo e del Consiglio, del 13 luglio 2009, che istituisce un codice comunitario dei visti (codice dei visti); GU L 243 del 15.9.2009, pag. 1.

Sensibilizzazione del pubblico

28. valutare l'opportunità di mettere opuscoli della DPA a disposizione degli interessati anche in luoghi più accessibili quali stazioni di polizia, zone adibite ai controlli di frontiera e sedi consolari;

29. considerare di rendere le presentazioni, i seminari e gli eventi a porte aperte della DPA accessibili anche al grande pubblico, in particolari agli interessati, i quali hanno bisogno di ricevere informazioni sul SIS II e sul VIS.

Fatto a Bruxelles, il

Per il Consiglio
Il presidente