Consiglio dell'Unione europea

Bruxelles, 14 maggio 2018
(OR. en)

8792/18

Fascicolo interistituzionale: 2018/0051 (NLE)

SCH-EVAL 102
COMIX 244

RISULTATI DEI LAVORI

Origine:	Segretariato generale del Consiglio
in data:	14 maggio 2018
Destinatario:	delegazioni
n. doc. prec.:	8285/18
Oggetto:	Decisione di esecuzione del Consiglio recante raccomandazione relativa alla correzione delle carenze riscontrate nella valutazione 2017 del **Portogallo** 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 2017 del Portogallo sull'applicazione dell'*acquis* di Schengen nel settore della protezione dei dati, adottata dal Consiglio nella sessione del 14 maggio 2018.

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.

ALLEGATO

Decisione di esecuzione del Consiglio recante

RACCOMANDAZIONE

relativa alla correzione delle carenze riscontrate nella valutazione 2017 del Portogallo 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 al Portogallo provvedimenti correttivi per colmare le carenze riscontrate durante la valutazione Schengen 2017 nel settore della protezione dei dati. A seguito della valutazione, con decisione di esecuzione della Commissione C(2018) 1190 è stata adottata una relazione riguardante i risultati e le valutazioni, che elenca le migliori pratiche e le carenze riscontrate.

(2) Per quanto riguarda le buone pratiche, l'equipe in loco si è felicitata degli investimenti continui operati dall'autorità per la protezione dei dati per la formazione del proprio personale tecnico.

[1] GU L 295 del 6.11.2013, pag. 27.

(3) In considerazione dell'importanza del rispetto dell'*acquis* di Schengen, in particolare dell'obbligo di garantire ed effettuare un controllo efficace e assicurare le necessarie misure di sicurezza, dovrebbe essere data priorità all'attuazione delle raccomandazioni 1, 4, 14, 17 e 22.

(4) È opportuno trasmettere la presente decisione al Parlamento europeo e ai parlamenti degli Stati membri. Entro tre mesi dalla sua adozione il Portogallo elabora, ai sensi dell'articolo 16, paragrafo 1, del regolamento (UE) n. 1053/2013, un piano d'azione volto a correggere le carenze riscontrate nella relazione di valutazione e lo presenta alla Commissione e al Consiglio,

RACCOMANDA che:

il Portogallo provveda a

Autorità di controllo per la protezione dei dati

1. assegnare all'autorità per la protezione dei dati sufficienti risorse finanziarie e umane per metterla in grado di svolgere tutti i compiti ad essa affidati a norma dell'*acquis* relativo al sistema d'informazione Schengen II (SIS II) e al sistema di informazione visti (VIS), anche in vista di un futuro aumento delle responsabilità;

2. al fine di garantire meglio la piena indipendenza dell'autorità per la protezione dei dati, assicurare alla stessa l'autonomia finanziaria per dare esecuzione al suo bilancio annuale e l'autonomia in materia di assunzione del personale, quantomeno allineando le relative norme a quelle applicabili ad altre autorità indipendenti in Portogallo;

3. assicurarsi che l'autorità per la protezione dei dati completi in tempi rapidi le procedure di adozione delle relazioni che fanno seguito alle ispezioni relative al trattamento dei dati personali in ambito SIS II;

4. assicurarsi che l'autorità per la protezione dei dati completi in tempi rapidi l'audit del VIS;

Diritti degli interessati

5. assicurarsi che sul sito web del Serviço de Estrangeiros e Fronteiras (servizio Immigrazione e frontiere) siano date informazioni agli interessati in merito ai loro diritti in relazione al SIS II;

6. assicurarsi che gli interessati che presentano domanda di accesso ai loro dati personali siano informati in merito alle categorie di dati effettivamente trattate nel SIS II;

7. assicurarsi che gli interessati ricevano informazioni chiare sull'identità del titolare del trattamento dei loro dati personali nella procedura di rilascio dei visti Schengen;

Sistema di informazione visti

8. chiarire la situazione per quanto riguarda la titolarità del trattamento dei dati personali nell'ambito dell'N.VIS (comprese le applicazioni usate dal ministero degli Affari esteri, dal servizio Immigrazione e frontiere e dai relativi centri dati), in particolare precisando il ruolo del ministero degli Affari esteri e la ripartizione delle responsabilità tra il servizio Immigrazione e frontiere e il ministero degli Affari esteri per quanto riguarda il trattamento dei dati personali;

9. assicurarsi che il ministero degli Affari esteri svolga attività di controllo sistematiche che consentano una significativa valutazione degli aspetti relativi al trattamento dei dati personali da parte del fornitore esterno di servizi. A tale riguardo il Portogallo è invitato ad ampliare il questionario che il ministero degli Affari esteri invia al fornitore esterno di servizi per affrontare in modo più dettagliato gli aspetti della protezione dei dati e potenziare le attività di controllo del ministero degli Affari esteri in relazione alla protezione dei dati operata dal fornitore esterno di servizi e dall'eventuale subcontraente;

10. definire una procedura che consenta la verifica degli hit nel SIS II nel corso della procedura di rilascio dei visti;

11. assicurarsi che tutte le password degli utenti N.VIS siano criptate;

12. assicurarsi che il servizio Immigrazione e frontiere e il ministero degli Affari esteri analizzino periodicamente i file di registro (log) per garantire il monitoraggio della protezione dei dati;

13. assicurarsi che il ministero degli Affari esteri effettui periodicamente l'automonitoraggio del trattamento dei dati personali nella Rede de Pedidos de Vistos (rete di domande di visto) e nel relativo centro dati;

14. assicurarsi che il ministero degli Affari esteri adotti in tempi rapidi un piano di sicurezza per la rete di domande di visto e il relativo centro dati;

15. dare piena attuazione alla decisione 2008/633/GAI del Consiglio, del 23 giugno 2008, relativa all'accesso per la consultazione al sistema di informazione visti (VIS) da parte delle autorità designate degli Stati membri e di Europol ai fini della prevenzione, dell'individuazione e dell'investigazione di reati di terrorismo e altri reati gravi e assicurarsi che l'accesso ai dati N.VIS rispetti i requisiti e la procedura stabiliti dalla decisione;

16. assicurarsi che il fornitore esterno di servizi cancelli i dati personali dei richiedenti registrati nei suoi sistemi nel rispetto dei termini previsti all'allegato X, parte A, lettera d), del codice dei visti, il quale impone di cancellare tali dati immediatamente dopo la loro trasmissione al consolato;

Sistema di informazione Schengen II

17. disporre l'istituzione di un sito di riserva completo per l'N.SIS II che disponga di tutte le funzionalità, compresa la connessione con l'infrastruttura di comunicazione s-Testa;

18. chiarire le responsabilità tra le parti che intervengono nel trattamento dei dati dell'N.SIS II, ovvero il titolare del trattamento e le autorità che hanno accesso al SIS.II (autorità utenti), per quanto riguarda la sicurezza informatica, il controllo e l'automonitoraggio in tale ambito, ad esempio mediante accordi tra il titolare del trattamento e le autorità che accedono al SIS II;

19. attuare una gestione utente che permetta di effettuare un efficace automonitoraggio sulla base dei file di registro (log) centrali da parte del titolare del trattamento N.SIS II senza bisogno di consultare i file di registro delle autorità utenti;

20. assicurarsi che il servizio Immigrazione e frontiere analizzi periodicamente i file di registro (log) per garantire il monitoraggio della protezione dei dati;

21. assicurarsi che gli ambienti informatici impiegati dagli utenti con diritti di amministratore o ampio accesso all'N.SIS (quali i membri dell'ufficio SIRENE) siano logicamente o fisicamente separati dall'accesso a internet;

22. assicurarsi che il titolare del trattamento proceda a crittografare i nastri di backup e i dischi rigidi dell'N.SIS;

23. assicurarsi che i profili degli utenti con diritti di amministratore o ampio accesso all'N.SIS (quali i membri dell'ufficio SIRENE) siano protetti mediante un sistema obbligatorio di autenticazione a due fattori;

24. assicurarsi che il servizio Immigrazione e frontiere incrementi le proprie attività relative all'automonitoraggio del trattamento dei dati personali nell'N.SIS ed esegua periodicamente tale automonitoraggio; il Portogallo è invitato a destinare al servizio Immigrazione e frontiere risorse umane e finanziarie sufficienti per garantire che il controllo interno e la sicurezza informatica siano efficaci e continui, in particolare facendo in modo che sia coperto il posto di addetto alla sicurezza informatica nella divisione "tecnologie dell'informazione" del servizio Immigrazione e frontiere;

Sensibilizzazione del pubblico

25. assicurarsi che il sito web del servizio Immigrazione e frontiere contenga collegamenti adeguati al sito web dell'autorità per la protezione dei dati.

Fatto a Bruxelles, il

Per il Consiglio
Il presidente