Direttiva del DFGP sull'installazione di collegamenti online e il rilascio di autorizzazioni d'accesso ad applicazioni informatiche del DFGP

(Direttiva online DFGP)

del 30 settembre 2004

Il Dipartimento federale di giustizia e polizia,
visto l'articolo 38 della legge federale del 21 marzo 1997¹ sull'organizzazione
del Governo e dell'Amministrazione (LOGA),
ordina:

Sezione 1: Generalità

Art. 1 Scopo

¹ La presente direttiva armonizza la procedura applicabile all'installazione di collegamenti online nel Dipartimento federale di giustizia e polizia (DFGP).

² Essa regola:

- a. la procedura e le condizioni per l'installazione di un collegamento online tra il DFGP e gli organi della Confederazione e dei Cantoni con il quale gli impiegati di questi organi (utenti) ottengono l'accesso a un'applicazione informatica del DFGP attraverso una procedura di richiamo;
- b. la procedura e le condizioni per il rilascio di autorizzazioni d'accesso individuali o collettive a questi utenti quando sono resi loro accessibili dati personali mediante il collegamento online.

Art. 2 Condizioni

Le condizioni per installare un collegamento online tra un'applicazione informatica del DFGP e gli utenti sono:

- a. l'esistenza di una base legale sufficiente ai sensi dell'articolo 19 capoverso 3 della legge federale del 19 giugno 1992² sulla protezione dei dati (LDP), che definisce concretamente le autorizzazioni per l'accesso e le condizioni quadro indispensabili (art. 3);
- b. l'utilizzazione vincolata (art. 4);
- c. la sicurezza del collegamento online (art. 5);

¹ RS 172.010

² RS 235.1

- d. una domanda della competente autorità cantonale quando l'installazione di un collegamento online riguarda un servizio cantonale (art. 16).

Sezione 2: Principi applicabili all'installazione di un collegamento online

Art. 3 Base legale

Un collegamento online necessita di una base legale esplicita. Se il collegamento online permette di accedere a dati personali degni di particolare protezione o a profili della personalità, è necessaria una legge formale.

Art. 4 Utilizzazione vincolata

¹ Un collegamento online può essere installato soltanto se utilizzato per gli scopi previsti dalla base legale.

² Se nella base legale lo scopo è descritto soltanto in termini generali, occorre precisarlo nella domanda d'installazione di un collegamento online.

Art. 5 Sicurezza

¹ Un collegamento online non può essere installato finché non sono stati garantiti il corretto trattamento dei dati e la loro sicurezza, vale a dire se sono adempiute le misure tecniche e organizzative di cui alla sezione 3.

² Un'infrastruttura di sicurezza centralizzata (SSO Portale DFGP³) controlla l'accesso a tutte le informazioni e applicazioni informatiche del DFGP. L'SSO Portale DFGP garantisce una gestione standardizzata e un'efficace autenticazione degli utenti.

Sezione 3: Misure tecniche e organizzative

Art. 6 Valutazione dei rischi

Prima della messa in esercizio di un'applicazione informatica con un collegamento online, l'ufficio federale responsabile dell'applicazione informatica effettua una valutazione dei rischi conformemente alle pertinenti direttive del Consiglio informatico della Confederazione (CIC) nonché dell'Organo strategia informatica della Confederazione (OSIC) e attua le misure che ne derivano.

³ Single-Sign-on Portale DFGP

Art. 7 Concetto di sicurezza dell'applicazione informatica

¹ Sulla base della valutazione dei rischi, l'ufficio federale responsabile dell'applicazione informatica allestisce un concetto di sicurezza informatica che preveda sufficienti misure tecniche e organizzative di protezione e sicurezza ai sensi dell'articolo 20 dell'ordinanza del 14 giugno 1993⁴ relativa alla legge federale sulla protezione dei dati (OLPD).

² Il concetto di sicurezza dell'applicazione informatica definisce segnatamente:

- a. i responsabili dell'applicazione;
- b. i responsabili della protezione dei dati;
- c. i responsabili della sicurezza informatica;
- d. l'organo di vigilanza;
- e. le regole applicabili alla verbalizzazione;
- f. la procedura d'identificazione e di autenticazione degli utenti;
- g. la codificazione dei dati;
- h. la procedura di rilascio delle autorizzazioni d'accesso;
- i. le regole e la procedura applicabili all'interruzione di collegamenti inattivi e al blocco di autorizzazioni d'accesso non sfruttati;
- j. la procedura di controllo ai sensi dell'articolo 9 capoverso 1 OLPD.

³ Il concetto di sicurezza dell'applicazione informatica è aggiornato periodicamente dall'ufficio federale responsabile.

⁴ Il rapporto finale dell'incaricato della sicurezza informatica del Dipartimento (ISID) e dell'Organo strategia informatica della Confederazione (OSIC) può sostituire il concetto di sicurezza dell'applicazione informatica se il regolamento per il trattamento menziona i punti di cui al capoverso 2.

Art. 8 Regolamento per il trattamento

Conformemente all'articolo 21 OLPD, gli uffici federali responsabili delle applicazioni informatiche emanano un regolamento per il trattamento delle loro applicazioni informatiche.

Sezione 4:
Condizioni per il rilascio di autorizzazioni d'accesso individuali

Art. 9 Idoneità

L'accesso online deve permettere di raggiungere gli obiettivi perseguiti.

⁴ RS 235.11

Art. 10 Necessità

¹ L'accesso online deve essere necessario all'adempimento di un compito stabilito dalla legge.

² L'autorizzazione d'accesso è ritenuta necessaria se l'adempimento di un compito senza il collegamento online richiederebbe un onere supplementare sproporzionato.

Art. 11 Proporzionalità

¹ L'accesso online deve essere proporzionale.

² È proporzionale se vi è un rapporto ragionevole tra l'ingerenza nella sfera personale della persona interessata e l'utilità auspicata di tale trattamento di dati.

³ L'autorizzazione d'accesso va limitata ai dati e alle funzioni necessari all'utente per l'adempimento dei compiti.

Art. 12 Criteri d'esame

All'atto della valutazione dei principi giusta gli articoli 9–11 sono determinanti segnatamente i seguenti criteri d'esame:

- a. la frequenza prevedibile dell'utilizzazione del singolo accesso;
- b. l'attuale frequenza di utilizzazione da parte dell'organo interessato;
- c. il numero di collaboratori dell'organo interessato che dispongono già di un diritto d'accesso;
- d. la portata dell'accesso accordato all'organo interessato;
- e. la necessità di agire in modo indipendente e rapido (ad es. al di fuori dei normali orari d'ufficio);
- f. la portata dell'accesso richiesto (criteri di ricerca, entità dei dati visualizzabili);
- g. le funzioni richieste (interrogazione, registrazione, mutazione, cancellazione).

Sezione 5: Organizzazione

Art. 13 Organo centrale di autenticazione

¹ L'organo centrale di autenticazione (servizio di autenticazione DFGP) è responsabile dell'autenticazione degli utenti che richiedono un accesso online ad applicazioni informatiche del DFGP. Gestisce l'SSO Portale DFGP.

² Riceve le domande d'accesso, procede all'autenticazione degli utenti e trasmette le domande all'ufficio federale responsabile dell'applicazione informatica.

³ Coordina la procedura per il rilascio di autorizzazioni d'accesso individuali.

Art. 14 Competenze in seno all'ufficio federale responsabile dell'applicazione informatica

¹ Il consulente per la protezione dei dati dell'ufficio federale responsabile dell'applicazione informatica (CPDU) vigila sulla pianificazione e sull'installazione dei collegamenti online e provvede affinché siano rispettate le regole relative al rilascio delle autorizzazioni d'accesso individuali.

² Esamina la prima domanda d'autorizzazione d'accesso individuale presentata da ogni organo della Confederazione o dei Cantoni e controlla il rispetto dei principi di cui alla sezione 4. Vigila, mediante sondaggio, affinché le successive autorizzazioni d'accesso individuali vengano rilasciate conformemente ai numeri 9–12.

³ Esamina l'esattezza e la completezza del regolamento per il trattamento.

⁴ L'incaricato della sicurezza informatica dell'unità amministrativa (ISI-U) è responsabile dell'esame degli aspetti legati alla sicurezza informatica. Controlla segnatamente se le misure di sicurezza sono conformi alle condizioni di cui agli articoli 6 e 7.

Art. 15 Fornitore di prestazioni dell'applicazione informatica

Il fornitore di prestazioni di ogni applicazione informatica è competente per la realizzazione tecnica dei collegamenti online se le autorizzazioni d'accesso individuali sono state rilasciate.

Sezione 6: Procedura per l'installazione di un collegamento online

Art. 16 Domanda della competente autorità cantonale

La competente autorità cantonale inoltra la domanda per l'installazione di un collegamento online all'ufficio federale responsabile dell'applicazione informatica. La domanda deve contenere:

- a. il nome degli organi per i quali chiede l'installazione di un collegamento online;
- b. il nome dell'applicazione informatica per la quale questi organi necessitano un collegamento online;
- c. lo scopo per il quale il collegamento va installato purché nella base legale esso sia descritto soltanto in termini generali.

Art. 17 Esame della domanda per l'installazione di un collegamento online

¹ Il CPDU esamina la domanda segnatamente per quanto concerne:

- a. la presenza di una base legale sufficiente;
- b. l'utilizzazione vincolata;
- c. le domande d'autorizzazione d'accesso collettive.

² Una volta accettata la domanda, trasmette il regolamento per il trattamento dell'applicazione informatica all'autorità cantonale richiedente.

Sezione 7:

Procedura per il rilascio di autorizzazioni d'accesso online individuali

Art. 18 Domanda d'accesso

¹ La domanda di rilascio per un accesso individuale va inoltrata con un modulo DFGP disponibile su Internet o Intranet.

² La domanda va inviata elettronicamente al servizio di autenticazione DFGP.

Art. 19 Esame delle domande di rilascio di un'autorizzazione d'accesso online

¹ L'ufficio federale responsabile dell'applicazione informatica esamina le domande d'autorizzazione d'accesso online individuali secondo i principi di cui alla sezione 4.

² Il CPDU esamina la prima domanda individuale presentata da un organo della Confederazione o dei Cantoni. Controlla, mediante sondaggio, le autorizzazioni d'accesso individuali rilasciate successivamente a un'utente appartenente al medesimo organo.

³ L'ufficio federale responsabile dell'applicazione informatica designa le persone abilitate a esaminare le successive domande d'autorizzazione. Può delegare l'esame a organi cantonali.

Art. 20 Autorizzazioni d'accesso collettive

¹ Un'autorizzazione d'accesso collettiva permette a tutti gli utenti appartenenti al medesimo gruppo di utilizzare gli stessi parametri d'identificazione (login di gruppo) quando si annunciano all'SSO Portale DFGP e alle applicazioni informatiche del DFGP.

² Un'autorizzazione d'accesso collettiva può essere rilasciata a una determinata categoria di utenti se sono adempiute le condizioni di cui alla sezione 4. Inoltre devono essere adempiute le condizioni seguenti:

- a. la stazione di lavoro è utilizzata in continuazione;
- b. il collegamento con un'applicazione deve essere stabilito molto rapidamente poiché l'accesso è urgente;
- c. la stazione di lavoro può essere utilizzata da tutti i componenti del gruppo di utenti menzionato nella domanda d'accesso;
- d. i titolari di autorizzazioni collettive possono soltanto consultare i dati nel rispettivo sistema informatico;
- e. i piani dei turni del gruppo di utenti sono conservati durante un anno;

- f. l'elenco dei componenti del gruppo di utenti è consegnato al responsabile dell'applicazione; e
- g. le mutazioni nel gruppo di utenti sono annunciati due volte l'anno al responsabile dell'applicazione;

Art. 21 Vigilanza

Il CPDU esamina periodicamente se gli accessi accordati sono conformi ai principi di cui alla sezione 4.

Sezione 8: Disposizioni finali

Art. 22 Disposizioni esecutive

La presente direttiva figura in allegato ed è parte integrante dei regolamenti per il trattamento di ogni applicazione informatica del DFGP con collegamenti online.

Art. 23 Disposizioni transitorie

¹ Le autorizzazioni d'accesso individuali esistenti al momento dell'entrata in vigore della presente direttiva restano valide fino all'introduzione di un'efficace autenticazione degli utenti. A tale momento saranno esaminate le autorizzazioni d'accesso individuali conformemente all'articolo 19.

² Quando un'applicazione informatica esistente è sostituita con una nuova, le autorizzazioni per l'installazione di un collegamento online (art. 17) conservano la loro validità.

³ Fino all'introduzione della firma elettronica nel DFGP è imperativo inviare per posta o fax al Servizio di autenticazione DFGP una copia firmata della domanda d'accesso (art. 18 cpv. 1).

⁴ Il DFGP trasmette entro il 31 dicembre 2004 i regolamenti per il trattamento delle applicazioni informatiche accessibili online il 31 agosto 2004 alle autorità cantonali responsabili degli organi dei Cantoni che vi sono collegati.

Art. 24 Entrata in vigore

La presente direttiva entra in vigore il 1° ottobre 2004.

30 settembre 2004

Dipartimento federale di giustizia e polizia:
Christoph Blocher