INFORMAZIONI AGLI UTENTI TITOLARI IDENTITÀ DIGITALE SPID: RISCHI, CAUTELE E CONTROMISURE

INDICE

1. INTRODUZIONE

L'art. 64 del D.Lgs. 7 marzo 2005 n. 82 e ss.mm.ii. (Codice dell'Amministrazione Digitale - di seguito anche solo "CAD") rubricato "*Sistema pubblico per la gestione delle identità digitali e modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni*" al fine di favorire la diffusione di servizi in rete e agevolare l'accesso a questi da parte di cittadini e imprese ha istituito, a cura dell'Agenzia per l'Italia Digitale (AgID), il "*sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID)*".

Al fine di consentire ai soggetti pubblici e privati di identificare gli utenti per consentire loro l'accesso ai servizi in rete l'AgID ha emanato apposito regolamento recante le "*modalità per l'accreditamento e la vigilanza dei gestori dell'identità digitale (articolo 1, comma 1, lettera l), dpcm 24 ottobre 2014)*".

Ai sensi dell'Allegato "*Documentazione per l'accreditamento*", paragrafo 2 "*Documenti tecnici e organizzativi generali*" " lett. ff) del regolamento sopra citato, il soggetto che intende accreditarsi presenta "*le informazioni fornite ai titolari dell'identità digitale SPID inerenti i rischi derivanti dal possesso della stessa, le cautele e le contromisure adottabili dagli stessi".*

1.1. SCOPO DEL DOCUMENTO

Lo scopo del presente documento (di seguito anche solo "*Informativa*"), ad uso Pubblico, è quello di TeamSystem S.p.a. - in qualità di "Gestore dell'identità digitale" così come definito ai sensi dell'art. 1 co. 1 lett. l) del D.P.C.M. 24 ottobre 2014 (di seguito anche solo "TeamSystem") - di informare i titolari dell'identità digitale SPID (di seguito anche solo "Titolari") circa i rischi derivanti dal possesso della stessa e le cautele e le contromisure adottabili dagli stessi per prevenirli.

1.2. RIFERIMENTI DELL'ORGANIZZAZIONE

Di seguito sono indicati i dati societari dell'organizzazione TeamSystem S.p.a. e relativi contatti:

Ragione Sociale: TeamSystem S.p.A. (Società per Azioni).

Partita Iva: 01035310414

Sede legale: Via Sandro Pertini, 88 - 61122 Pesaro (PU)

Tel: 0721 42661

Sito internet: https://www.teamsystem.com/

1.3. GLOSSARIO E DEFINIZIONI

All'interno del documento si fa riferimento alle definizioni riportate nella tabella che segue; per ogni termine non contenuto all'interno della tabella si rimanda alle definizioni di cui all'art. 1 del D.P.C.M. 24 ottobre 2014 nonché al Regolamento GDPR.

AgID	Agenzia per l'Italia Digitale
CAD	Codice dell'Amministrazione Digitale (D.Lgs. 7 marzo 2005 n. 82 e ss.mm.ii.)
DPCM	Decreto del Presidente del Consiglio dei Ministri del 24 ottobre 2014 recante "Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese".
IdP	"Identity Provider" – "Gestore dell'Identità Digitale": persona giuridica che ha ottenuto l'accreditamento da AgID per l'attività di rilascio e gestione delle credenziali SPID.
GDPR	Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016
Codice Privacy	Decreto Legislativo 30 giugno 2003, n. 196 recante il "Codice in materia di protezione dei dati personali" così come integrato dal Decreto Legislativo 10 agosto 2018, n. 101, recante "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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)".*
Richiedente	Persona fisica o giuridica che richiede il rilascio di credenziali di autenticazione SPID (di livello 1, 2 o 3)
Manuale Operativo	Il Manuale Operativo di TeamSystem S.p.a. relativo ai servizi di gestione del servizio SPID
Informativa	Il presente documento
Titolare/Utente	Persona fisica o giuridica titolare delle credenziali di autenticazione SPID (di livello 1, 2 o 3)
Service Provider (SP)/Fornitori di servizi	Soggetti pubblici o privati che erogano i propri servizi on-line previa autenticazione dell'utente tramite le credenziali SPID dell'IdP
Identificazione Informatica	L'identificazione di cui all'art. 1 co. 1 lett. u-ter) del Decreti legislativo 7 marzo 2005 n. 82 (CAD)

Identità Digitale	Rappresentazione informatica della corrispondenza biunivoca tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale secondo le modalità di cui al presente decreto e dei suoi regolamenti attuativi
SPID	Il Sistema pubblico dell'identità digitale, istituito ai sensi dell'art. 64 del CAD, modificato dall'art. 17-ter del decreto-legge 21 giugno 2013, n. 69, convertito, con modificazioni, dalla legge 9 agosto 2013, n. 98
Regolamento SPID	Regolamento recante le modalità attuative per la realizzazione dello SPID (articolo 4, comma 2, DPCM 24 ottobre 2014) emesso da AgID
Registrazione	L'insieme delle procedure informatiche, organizzative e logistiche mediante le quali, con adeguati criteri di gestione e protezione previsti dal presente decreto e dai suoi regolamenti attuativi, è attribuita un'identità digitale a un utente, previa raccolta, verifica e certificazione degli attributi da parte del gestore dell'identità digitale, garantendo l'assegnazione e la consegna delle credenziali di accesso prescelte in modalità sicura

2. RISCHI DELL'IDENTITA' DIGITALE SPID

2.1 RESPONSABILITA' DEL TITOLARE

Ai fini del rilascio, da parte di TeamSystem, dell'identità digitale tramite SPID, il Richiedente è tenuto a compilare e sottoscrivere un modulo di richiesta di adesione contenente, ai sensi dell'art. 5 del Regolamento SPID, tutte le informazioni necessarie per la sua corretta identificazione.

Con la sottoscrizione del modulo il Richiedente, futuro Titolare delle credenziali di autenticazione tramite SPID, si impegna anche al rispetto di un insieme di regole ed obblighi normativi e/o regolamentari oltre che impegnarsi al rispetto del Manuale Operativo relativo ai servizi di autenticazione tramite SPID di TeamSystem.

In tali documenti sono messi in luce i rischi a cui quest'ultimo va incontro con il rilascio della predetta identità.

2.1.1. OBBLIGHI DEL TITOLARE AI FINI DEL RILASCIO DELL'IDENTITA' DIGITALE

Il Titolare, all'atto della presentazione del Modulo di richiesta di adesione al servizio SPID, allo scopo di consentire a TeamSystem di dare esecuzione alla richiesta di identificazione e successivo rilascio dell'identità digitale:

- si assume la responsabilità, ai sensi del d.P.R. 28 dicembre 2000 n. 445, della veridicità delle informazioni inserite nel modulo di richiesta di adesione;
- prende visione e presta il consenso all'Informativa redatta ai sensi dell'art. 13 e 14 del GDPR;
- si impegna a rispettare le disposizioni contenute nel Manuale Operativo di TeamSystem la cui consultazione è consentita in fase di compilazione del modulo di richiesta di adesione nonché in qualunque momento;
- dichiara di accettare ogni condizione riportata nel modulo di richiesta di adesione a SPID, che riveste a tutti gli effetti valenza contrattuale;
- dichiara, previa visione, di accettare le condizioni generali del servizio di autenticazione tramite SPID di TeamSystem;
- si impegna a fornire a TeamSystem ogni informazione richiesta ai fini dell'esecuzione del Servizio SPID e dei correlati necessari controlli; inoltre, il Titolare si impegna a

comunicare ogni modifica dei dati identificativi forniti in fase di registrazione, come previso dal Manuale Operativo.

2.1.2. OBBLIGHI DEL TITOLARE SUCCESSIVI AL RILASCIO DELL'IDENTITA' DIGITALE

Il Titolare in possesso dell'identità digitale (di Livello 1 o 2) rilasciata da TeamSystem, inoltre:

- si assume ogni responsabilità, nel limite massimo consentito dalla legge, ove si verifichi un utilizzo improprio o non conforme delle credenziali a quanto previsto dalla normativa vigente e dal Manuale Operativo. Al riguardo, il Titolare esonera TeamSystem da qualsiasi richiesta dovesse pervenire da parte di terzi;
- consapevole di quanto previsto ai sensi del codice penale e delle leggi speciali in materia (Decreto 445/2000) in materia di punibilità delle dichiarazioni mendaci, conferma e dà garanzia della veridicità di tutti i dati personali e del numero di telefono cellulare comunicati all'atto dell'identificazione;
- è tenuto ad usare esclusivamente e personalmente le credenziali proprie dell'Identità Digitale e, al contempo, ha l'onere di provare l'utilizzo abusivo di queste da parte di terzi;
- si impegna a non fare un uso improprio delle credenziali (violando leggi o regolamenti), al fine di arrecare danni alla rete o a terzi. Il Titolare si impegna, pertanto, a mettere in atto ogni forma organizzativa e tecnica finalizzata a evitare danni ai terzi.

In aggiunta agli obblighi di cui sopra, il Titolare:

- si vincola a conservare nella maniera più diligente possibile le credenziali di autenticazione che gli sono state attribuite, ad utilizzare in maniera esclusiva tanto le credenziali di accesso quanto gli eventuali dispositivi annessi, impegnandosi o non permettere l'utilizzo a terzi;
- ove dovesse smarrire o gli dovessero essere sottratte le credenziali, si vincola a sporgere immediatamente denuncia alle Autorità competenti e a fornire tempestivamente copia della denuncia a TeamSystem;
- si impegna ad aggiornare in autonomia o su segnalazione del Gestore i seguenti dati personali: estremi e scadenza del documento di riconoscimento; numero di telefono; indirizzo di posta elettronica; indirizzo di domicilio tanto fisico quanto digitale;
- si impegna a conservare tanto le credenziali quanto le informazioni necessarie per

l'utilizzo dell'Identità digitale in modo da ridurre al minimo ogni tipo di rischio;

- in caso di necessità, si impegna a chiedere l'immediata sospensione e/o revoca delle Credenziali nei casi e con le modalità previste nel Manuale Operativo.

2.1.3. ULTERIORI OBBLIGHI

Inoltre, il Titolare resta direttamente ed esclusivamente responsabile per tutti gli eventi connessi all'utilizzo delle credenziali, fino all'effettiva eventuale sospensione, revoca del servizio o recesso dal medesimo.

Il Titolare si impegna a non utilizzare le credenziali di autenticazione al fine di compiere atti suscettibili di ledere diritti altrui (a titolo esemplificativo diritti di autore e più in generale ogni altro diritto ritenuto meritevole di tutela dalla legge).

In caso di violazione di anche una sola delle presenti disposizioni, TeamSystem potrà risolvere il contratto senza obbligo di preavviso, o risarcimento di alcun danno, con esclusione di ogni eventuale azione di rivalsa da porre in essere nei riguardi dei responsabili delle violazioni.

3. CAUTELE E CONTROMISURE A TUTELA DELL'IDENTITA' DIGITALE SPID

3.1. CASI DI ACCESSO NON AUTORIZZATO

Nel presente paragrafo sono descritte parte delle conseguenze che si verificano a seguito di un accesso non autorizzato ovvero di una violazione dell'accesso o di un uso improprio delle credenziali di autenticazione tramite SPID.

L'accesso non autorizzato si verifica nel momento in cui un terzo, in possesso delle credenziali di autenticazione SPID del Titolare, tenta di effettuare l'accesso ad un *Service Provider* inserendo le predette credenziali.

In tali casi si possono verificare le seguenti circostanze a seconda del "Livello" della credenziale di autenticazione illegittimamente utilizzata:

- **Livello 1**: dal momento che il livello 1 di credenziali SPID prevede unicamente l'inserimento di una *username* e di una *password*, il terzo, che sia in possesso di tali credenziali può accedere ai servizi on-line dei *Service Provider* che supportano esclusivamente tale livello di autenticazione;
- **Livello 2**: il livello di autenticazione maggiormente utilizzato dai *Service Provider* in quanto prevede un meccanismo di autenticazione a due fattori, molto più sicuro: infatti, qualora il terzo, in possesso delle credenziali SPID del Titolare, provi ad effettuare l'accesso ad una piattaforma che richieda lo SPID di Livello 2, non riuscirà ad accedere, dal momento che l'ulteriore passaggio richiesto è l'inserimento di un'ulteriore credenziale (codice OTP recapitato tramite SMS) cui difficilmente il terzo può entrare in possesso;

Inoltre, ogni volta che il Titolare completerà con successo un'autenticazione presso un Service Provider, riceverà da parte di TeamSystem una notifica, via email, di avvenuto accesso. Questa notifica è essenziale e deve essere costantemente monitorata da parte del Titolare al fine di accorgersi immediatamente di eventuali accessi da lui non autorizzati e potersi attivare conseguentemente.

3.2. AZIONI DA INTRAPRENDERE IN CASO DI ACCESSO NON AUTORIZZATO

Nei casi descritti nel paragrafo precedente, ove si determini una violazione dell'accesso, il Titolare è tenuto a richiedere, tempestivamente, ai sensi di quanto indicato nel Manuale

operativo, l'intervento di TeamSystem, che a sua volta procede con la revoca o la sospensione dell'identità digitale rilasciata.

Proprio la rapidità, tanto del Titolare quanto di TeamSystem, sono fondamentali per consentire di evitare o ridurre i rischi per il Titolare conseguenti ad un utilizzo improprio dell'identità.

Al fine di contenere le criticità e i rischi enunciati nel precedente paragrafo, a cui il Titolare dell'identità digitale SPID può andare incontro, vi sono una serie di cautele e contromisure che quest'ultimo può adottare, riportate schematicamente di seguito:

AMBITO DI APPLICAZIONE:	**CAUTELE E CONTROMISURE DA PORRE IN ESSERE:**
CELLULARE	Inibire l'anteprima degli SMS per evitare che il codice SPID possa essere letto.
	Istallare solo applicazioni acquisite da canali ufficiali.
	Impostare il blocco dello schermo del cellulare, a tutela in caso di furto.
	Aggiornare frequentemente il dispositivo
	Ripristinare il sistema dello smartphone ove non più in utilizzo.

COMPUTER	Installare ed attivare Antivirus sul computer.
	Impostare in automatico l'aggiornamento del sistema operativo.
	Effettuare sempre il Logout dall'identità digitale e cancellare ogni traccia della connessione una volta conclusa l'operazione.
IMPOSTAZIONE DEI DATI PASSWORD	Modificare frequentemente la password legata all'identità digitale.
	Attivare l'opzione di segnalazione dell'utilizzo della identità digitale a mezzo mail di notifica, così da avere contezza di usi impropri.
	Conservare gelosamente la password e non divulgarla a terzi
	Utilizzare una password nuova dedicata esclusivamente all'identità digitale.
	Provvedere al salvataggio di indirizzo e-mail e telefono cellulare connessi all'identità digitale.