Parere sullo schema di decreto relativo alla piattaforma digitale per l’erogazione di benefici economici concessi dalle amministrazioni pubbliche, da adottarsi, di concerto con il Ministro dell’economia e delle finanze, ai sensi dell’art. 28-bis, comma 3, del d.l. 6 novembre 2021, n. 152, convertito, con modificazioni, dalla l. 29 dicembre 2021, n. 233 - 28 luglio 2022 [9809029]

VEDI ANCHE NEWSLETTER DEL 3 OTTOBRE 2022

[doc. web n. 9809029]

Parere sullo schema di decreto relativo alla piattaforma digitale per l’erogazione di benefici economici concessi dalle amministrazioni pubbliche, da adottarsi, di concerto con il Ministro dell’economia e delle finanze, ai sensi dell’art. 28-bis, comma 3, del d.l. 6 novembre 2021, n. 152, convertito, con modificazioni, dalla l. 29 dicembre 2021, n. 233 - 28 luglio 2022

Registro dei provvedimenti
n. 286 del 28 luglio 2022

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzione, presidente, il dott. Agostino Ghiglia e l’avv. Guido Scorza, componenti, e il cons. Fabio Mattei, segretario generale;

VISTO il 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 – di seguito “Regolamento”);

VISTO il d.lgs. 30 giugno 2003, n. 196, recante “Codice in materia di protezione dei dati personali” (di seguito “Codice”);

VISTA la documentazione in atti;

VISTE le osservazioni formulate dal segretario generale ai sensi dell’art. 15 del regolamento del Garante n. 1/2000;

RELATORE l’avv. Guido Scorza;

PREMESSO

Il Ministro per l’innovazione tecnologica e la transizione digitale, con nota del 27 giugno 2022, ha

chiesto il parere del Garante sullo schema di decreto relativo alla piattaforma digitale per l'erogazione di benefici economici concessi dalle amministrazioni pubbliche (di seguito "piattaforma"), da adottarsi, di concerto con il Ministro dell'economia e delle finanze, ai sensi dell'art. 28-bis, comma 3, del d.l. 6 novembre 2021, n. 152, convertito, con modificazioni, dalla l. 29 dicembre 2021, n. 233.

1. Il quadro normativo.

Il richiamato art. 28-bis del d.l. 152/2021 stabilisce, in primo luogo, che "nell'ambito dell'intervento "Servizi digitali e cittadinanza digitale" del Piano nazionale per gli investimenti complementari, […] al fine di incentivare la digitalizzazione dei pagamenti della pubblica amministrazione, di uniformare i processi di erogazione dei benefìci economici concessi dalle amministrazioni pubbliche e di consentire un più efficiente controllo della spesa pubblica, i benefìci economici concessi da un'amministrazione pubblica di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, a favore di persone fisiche o giuridiche residenti nel territorio dello Stato e destinati a specifici acquisti da effettuare attraverso terminali di pagamento (POS) fisici o virtuali possono essere erogati, nel limite delle risorse disponibili a legislazione vigente, mediante utilizzo della piattaforma tecnologica prevista all'articolo 5, comma 2, del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82" (comma 1).

A questo fine, "i servizi di progettazione, di realizzazione e di gestione del sistema informatico destinato all'erogazione dei benefìci economici di cui al comma 1 sono svolti dalla società di cui all'articolo 8, comma 2, del decreto-legge 14 dicembre 2018, n. 135, convertito, con modificazioni, dalla legge 11 febbraio 2019, n. 12" (comma 2).

Inoltre, è previsto che "la struttura della Presidenza del Consiglio dei ministri competente per l'innovazione tecnologica e la transizione digitale comunica, con cadenza semestrale, al Ministero dell'economia e delle finanze, anche sulla base dei dati e delle informazioni rilevati dai sistemi di monitoraggio di cui all'articolo 1, comma 7, del decreto-legge 6 maggio 2021, n. 59, convertito, con modificazioni, dalla legge 1° luglio 2021, n. 101, le risorse utilizzate, lo stato di attuazione degli interventi e gli obiettivi conseguiti" (comma 4), e che "il Ministero dell'economia e delle finanze stipula, a titolo non oneroso, una o più convenzioni con la società di cui all'articolo 8, comma 2, del decreto-legge 14 dicembre 2018, n. 135, convertito, con modificazioni, dalla legge 11 febbraio 2019, n. 12, al fine di definire le modalità e i tempi di comunicazione dei flussi contabili relativi ai benefìci di cui al comma 1 del presente articolo nonché le modalità di accreditamento dei medesimi benefìci" (comma 5).

Per dare attuazione a tale previsione normativa, il comma 3 stabilisce che "con uno o più decreti del Presidente del Consiglio dei ministri o del Ministro per l'innovazione tecnologica e la transizione digitale, di concerto con il Ministro dell'economia e delle finanze, sentito il Garante per la protezione dei dati personali per gli aspetti di competenza, sono definiti il cronoprogramma procedurale per la progettazione e la realizzazione dell'infrastruttura tecnologica per l'erogazione dei benefìci di cui al presente articolo, nonché le modalità di attuazione del medesimo articolo, comprese le modalità di funzionamento della piattaforma di cui al comma 1, stabilendo, in particolare, le modalità di colloquio con i sistemi informativi utilizzati dalle amministrazioni pubbliche per la gestione contabile della spesa, di erogazione e di fruizione uniformi dei benefìci, di verifica del rispetto dei limiti delle risorse disponibili a legislazione vigente, nonché di remunerazione del servizio da parte delle amministrazioni pubbliche che intendono avvalersene al fine di coprire i costi di gestione della piattaforma e di garantirne l'autosostenibilità a regime", mentre "le amministrazioni pubbliche di cui al citato articolo 1, comma 2, del decreto legislativo n. 165 del 2001 determinano i casi di utilizzo della piattaforma di cui al comma 1 del presente articolo, nel rispetto delle modalità di funzionamento stabilite dal decreto di cui al primo periodo del presente comma".

2. Lo schema di decreto in esame.

Lo schema di decreto in esame, da adottarsi ai sensi del richiamato art. 28-bis del d.l. 152/2021, nell'ambito delle definizioni rilevanti (art. 1), precisa, innanzitutto (comma 1, lett. n) e s)), che, in tale contesto, per "piattaforma" si intende l'infrastruttura tecnologica dedicata all'erogazione dei benefici economici concessi dalle amministrazioni pubbliche e sviluppata, ai sensi del citato art. 28-bis, dalla società di cui all'art. 8, comma 2, del d.l. 14 dicembre 2018, n. 135, convertito, con modificazioni, dalla l. 11 febbraio 2019, n. 12, ossia PagoPA S.p.A. (di seguito "PagoPA"), individuata quale "gestore della piattaforma" (di seguito anche "gestore").

Lo schema, in particolare, è volto a disciplinare "le modalità di attuazione e di funzionamento della stessa piattaforma per consentire, agli enti promotori, di erogare i benefici economici in favore dei relativi utenti, a condizione che tali benefici economici siano collegati ad acquisti effettuati attraverso i dispositivi di accettazione" (art. 2, comma 1).

Con riferimento all'infrastruttura tecnologica e alle modalità di funzionamento della piattaforma, viene previsto, tra le altre cose, che:

- il gestore della piattaforma stipuli:
  - accordi di adesione con gli enti promotori (ossia, ai sensi dell'art. 1, comma1, lett. l), le amministrazioni pubbliche che erogano i benefici economici attraverso la stessa, "ovvero la Ragioneria Generale dello Stato per le iniziative di sua competenza"), nei quali sono definite "le specifiche modalità di colloquio della piattaforma, per il tramite di interfacce informatiche, con i sistemi informativi degli stessi enti promotori per la gestione contabile della spesa, per l'erogazione e fruizione dei benefici nonché per la verifica del rispetto dei limiti delle risorse disponibili a legislazione vigente" (art. 3, comma 2);
  - una convenzione con il Ministero dell'economia e delle finanze in cui sono definiti "i meccanismi di comunicazione dei flussi contabili, che consentono la regolamentazione dei benefici erogati, con le interfacce messe a disposizione dalla Ragioneria Generale dello Stato" (art. 3, comma 9);
- la piattaforma sia composta da due componenti autonome che consentono di accedere ai benefici economici concessi dalle amministrazioni pubbliche per acquisti effettuati mediante due diverse tipologie di strumenti, la cui progettazione e realizzazione infrastrutturale sono eseguite in due fasi autonome e distinte, da effettuarsi nell'ordine di seguito indicato (art. 3, comma 5):
  - strumenti di pagamento (gli strumenti di pagamento utilizzati nell'ambito di operazioni di acquisto di beni o servizi per il tramite di un dispositivo di accettazione; art. 1, comma 1, lett. y));
  - strumenti di acquisto ("ogni strumento identificativo dell'utente che la piattaforma consenta di censire per partecipare ad un'iniziativa ed eseguire gli acquisti connessi alla iniziativa medesima tra cui la CIE, la tessera sanitaria, lo SPID o l'accesso all'app IO", art. 1, comma 1, lett. x));
- il gestore curi la manutenzione della piattaforma al fine di garantire il rispetto ogni standard tecnologico in materia di sicurezza e di tutela dei dati personali e provveda al suo aggiornamento tecnologico, nonché alla divulgazione delle sue specifiche tecniche ai soggetti coinvolti nell'erogazione del servizio (art. 3, comma 8), tra i quali rilevano, oltre agli enti promotori, anche:

gli acquirer convenzionati, ossia i soggetti che hanno concluso accordi con gli esercenti per l'utilizzo di dispositivi di accettazione (il dispositivo, il software e/o le applicazioni informatiche che consentono di effettuare acquisti utilizzando strumenti di pagamento o strumenti di acquisto, art. 1, comma 1, lett. j) e che hanno sottoscritto convenzioni con il gestore per partecipare al programma, ovvero la Bancomat S.p.A., previa sottoscrizione della convenzione con il gestore (art. 1, comma 1, lett. a));

gli issuer convenzionati, definendo come issuer "il soggetto che ha concluso un accordo con l'utente fruitore per la fornitura di uno strumento di pagamento elettronico e che ha sottoscritto una convenzione con PagoPA S.p.A. ovvero il soggetto che ha sottoscritto una convenzione con la stessa società per mettere a disposizione dei propri clienti, in alternativa all'app IO, un sistema per l'adesione ad un'iniziativa" (art. 1, comma 1, lett. q)).

Dopo aver definito le modalità di adesione degli enti promotori alla piattaforma e le modalità di configurazione di un'iniziativa da parte degli enti medesimi (artt. 4 e 5), lo schema si occupa poi di disciplinare l'accesso alla piattaforma e l'adesione alle iniziative per gli utenti, stabilendo, tra le altre cose, che:

"gli utenti fruitori, previa autenticazione con SPID o CIE, di livello di sicurezza almeno significativo, accedono alla piattaforma tramite App IO o altro canale messo a disposizione dal gestore della piattaforma ovvero, in alternativa, previa loro autenticazione da parte dell'issuer convenzionato tramite i canali fisici o digitali da quest'ultimo integrati con la piattaforma" (art. 6, comma 1); dopo essersi autenticato, l'utente fruitore, su base volontaria, "può aderire alle iniziative rese disponibili sulla piattaforma, registrare i propri strumenti di pagamento ovvero i propri strumenti di acquisto che la piattaforma consente di abilitare, registrare codici IBAN identificativi di conti correnti a lui intestati, nonché visualizzare tutte le informazioni relative alle iniziative a cui ha aderito" (art. 6, commi 3 e 4);

il gestore, "laddove l'utente registra una carta di debito o prepagata abilitata al circuito PagoBancomat, ottiene dalla società Bancomat S.p.A. gli estremi identificativi della carta di debito o prepagata in uso all'utente fruitore, mediante il codice fiscale fornito in sede di registrazione dall'utente medesimo" (art. 6, comma 5), mentre, "se l'utente registra uno strumento di acquisto, ottiene, mediante il codice fiscale fornito in sede di registrazione dallo stesso dall'Istituto Poligrafico e Zecca dello Stato S.p.A. i dati identificativi delle CIE e dall'Agenzia delle Entrate i dati identificativi della tessera sanitaria se non precedentemente disponibile all'interno dell'ecosistema di AppIO" (art. 6, comma 6); sono anche previste verifiche sulla qualità di legale rappresentante in caso di adesione ad un'iniziativa da parte di un utente persona giuridica (art. 6, comma 7);

per quanto concerne le verifiche sul possesso dei requisiti necessari alla partecipazione ad un'iniziativa da parte di un utente, queste possono essere effettuate "su richiesta dell'ente promotore, dal gestore della piattaforma mediante l'utilizzo del codice fiscale fornito in sede di registrazione alla piattaforma dall'utente fruitore, la piattaforma digitale nazionale dati di cui all'articolo 50-ter del CAD ovvero mediante la collaborazione con il soggetto giuridico che ha in gestione la banca dati recante le informazioni necessarie per la suddetta verifica" (art. 6, comma 8); "al fine di poter effettuare le verifiche di cui al comma 7", il gestore "è legittimato ad integrarsi con ogni ente in grado di fornirgli supporto nonché ad accedere alle informazioni dell'utente disponibili nelle relative banche dati" (art. 6, comma 9);

"l'utente, per aderire ad un'iniziativa, laddove abbia censito uno strumento di pagamento, memorizza, attraverso uno dei canali abilitanti, un IBAN identificativo di un conto corrente a lui intestato. La titolarità del conto in capo allo stesso utente è verificata dal gestore della piattaforma" (art. 6, comma 11); i canali abilitanti sono "l'App IO o altro canale messo a

disposizione dal gestore previa autenticazione mediante l'identità digitale di cui all'articolo 64, comma 2-quater, del CAD con livello di sicurezza almeno significativo a mezzo CIE o SPID con livello di sicurezza almeno significativo, e/o i canali fisici previa identificazione o quelli digitali messi a disposizione da uno issuer convenzionato ed integrati con la piattaforma, previa autenticazione da parte dello stesso issuer"(art. 1, comma 1, lett. e));

"l'utente può cancellare, in qualsiasi momento, attraverso i canali abilitanti, la propria adesione alla singola iniziativa o, più in generale, alla piattaforma"; la cancellazione dall'iniziativa determina, in particolare, "sia la perdita del diritto a concorrere all'assegnazione del beneficio secondo le regole dell'iniziativa fissate dall'ente promotore, sia la cancellazione di tutti i dati personali inerenti l'utente fruitore con riferimento alla singola iniziativa, fatta salva l'ipotesi in cui sussistano ulteriori basi giuridiche del trattamento, ivi inclusa quella di fare fronte a eventuali contestazioni o contenziosi" (art. 6, comma 12);

"Per agevolare la fruizione dei servizi da parte degli utenti, la piattaforma può inviare ai medesimi, ove siano utenti di app IO o di altri canali nella titolarità del gestore della piattaforma, ogni informazione utile in merito alle iniziative mediante servizi di messaggistica" (art. 6, comma 13), mentre l'utente può "indicare un recapito digitale tra quelli supportati dalla piattaforma, per ricevere le informazioni circa le iniziative a cui ha aderito" (art. 6, comma 14);

resta ferma "la facoltà dei singoli enti promotori di configurare un'iniziativa limitandola ad un numero determinato di utenti fruitori identificati dallo stesso ente promotore e comunicati al gestore della piattaforma ovvero di vietare l'adesione ad un numero determinato di utenti fruitori identificati dallo stesso ente promotore e comunicati al gestore della piattaforma" (art. 6, comma 15).

Per quanto concerne la partecipazione a un'iniziativa mediante l'utilizzo degli strumenti di pagamento, viene previsto, tra le altre cose, che:

l'utente accede ai benefici mediante uno degli strumenti di pagamento censiti sulla piattaforma da utilizzare presso gli esercenti, avendo la possibilità di "memorizzare piu IBAN che potranno essere utilizzati gradatamente, per l'accredito del beneficio, secondo l'ordine indicato dallo stesso utente" (art. 7, comma 1);

per l'erogazione di un beneficio, il gestore produce e invia all'ente promotore flussi informativi, predisposti sulla base dei flussi ricevuti dall'acquirer convenzionato che ha gestito la transazione, che determinano, con riferimento all'utente fruitore, l'accredito del beneficio maturato in un momento successivo rispetto al momento dell'acquisto (art. 7, commi 2 e 3);

l'esercente trasmette al gestore, per il tramite dell'acquirer convenzionato, i seguenti dati necessari alla piattaforma nella gestione delle iniziative (art. 7, comma 4):

il codice dello strumento di pagamento crittografato;

gli estremi della transazione con esito positivo inviata, ovvero i dati contenuti nella ricevuta elaborata dal dispositivo di accettazione anche in forma cartacea, tra cui la marca temporale del pagamento, l'importo della transazione espresso in euro egli identificativi univoci dell'operazione di pagamento che colleghino le fasi dell'operazione di pagamento stessa;

l'identificativo univoco dell'esercente, attribuito da ciascun acquirer;

l'identificativo fiscale dell'esercente;

il codice della categoria merceologica dell'esercente o il codice ATECO ovvero ogni altro codice disponibile a livello nazionale per la categorizzazione dell'esercente;

se l'iniziativa ha per oggetto specifici acquisti, l'esercente trasmette al gestore della piattaforma anche "il codice categoria del bene acquistato, per mezzo degli strumenti di accettazione, anche per il tramite dell'acquirer convenzionato" (art. 7, comma 5);

il gestore, sulla base delle regole di configurazione dell'iniziativa fissate dall'ente promotore, calcola l'importo del rimborso e predispone i flussi informativi utili all'ente promotore per procedere al rimborso nei confronti del beneficiario, che viene accreditato sul conto corrente individuato con l'IBAN indicato dall'utente (art. 7, comma 6);

la piattaforma mette, inoltre, a disposizione dell'ente promotore specifici report standard predisposti dal gestore della piattaforma, senza possibilità da parte dell'ente promotore di richiedere al gestore ulteriore reportistica a suo supporto (art. 7, comma 7, analogo al successivo art. 8, ultimo comma, relativo agli strumenti di acquisto).

Per quanto concerne, invece, la partecipazione a un'iniziativa mediante l'utilizzo degli strumenti di acquisto, viene stabilito, tra le altre cose, che:

a ogni utente è associato, per ciascuno strumento, un PIN specifico rilasciato dal gestore, attraverso i canali abilitanti gestiti da quest'ultimo, "al solo scopo di poter utilizzare tali strumenti di acquisto per la partecipazione alle iniziative" (art. 8, comma 1);

l'utente, al momento dell'acquisto presso un esercente, "si identifica" con uno strumento di acquisto e con il PIN specifico mediante il dispositivo di accettazione opportunamente configurato; tale dispositivo, per il tramite dell'acquirer convenzionato, invia la richiesta autorizzativa al gestore, trasmettendo le tipologie di informazioni indicate al citato art. 7, compreso, se applicabile, "il codice categoria del bene acquistato" (art. 8, commi 2 e 3);

"la piattaforma verifica in tempo reale il diritto dell'utente a uno o piu benefici. In caso di esito positivo autorizza, totalmente o parzialmente, a seconda delle regole fissate per l'iniziativa, l'importo dell'acquisto, permettendo all'esercente di concludere la fase di acquisto" (art. 8, comma 4);

il gestore, sulla base delle regole di configurazione dell'iniziativa fissate dall'ente promotore, calcola l'importo del rimborso spettante all'esercente e predispone i flussi informativi utili all'ente promotore per procedere al rimborso nei confronti dell'esercente, che viene accreditato per il tramite del relativo acquirer convenzionato o sul conto corrente di cui all'IBAN indicato dall'esercente per il tramite del medesimo acquirer (art. 8, comma 4 (rectius 5)).Gli acquirer convenzionati, previo accordo con il gestore, integrano i propri sistemi tecnologici con la piattaforma, "al fine di consentire la trasmissione dei dati relativi alle transazioni di pagamento per il funzionamento della piattaforma, comprese quelle gestite internamente (c.d. modalità on-us) e incluse le operazioni di storno o riaccredito"; in tal modo, agli esercenti è consentito di partecipare alle iniziative degli enti promotori, "con facoltà degli stessi esercenti di decidere se accettare solo strumenti di pagamento o anche strumenti di acquisto" (art. 9).

Infine, lo schema contiene specifiche disposizioni sul trattamento dei dati personali, le quali prevedono che:

"i dati personali raccolti ai sensi del presente decreto possono essere trattati esclusivamente per la finalità di cui all'articolo 2, comma 1" (art. 10, comma 8);

con riferimento ai ruoli ricoperti dai vari soggetti coinvolti nel trattamento:

ciascun ente promotore “è il titolare del trattamento dei dati personali necessari allo svolgimento di ogni iniziativa dallo stesso attivata e gestita mediante la piattaforma e si avvale del gestore della piattaforma in qualità di responsabile del trattamento” (art. 10, comma 1).;

il gestore “è il titolare del trattamento dei dati personali relativi all’utilizzo da parte dell’utente dell’AppIO o altro canale messo a disposizione dal gestore della piattaforma per aderire alle iniziative, nonché dei dati relativi agli strumenti di pagamento o di acquisto e agli IBAN registrati dall’utente”, mentre “agisce […] in qualità di responsabile del trattamento ai sensi dell'articolo 28 del Regolamento UE 2016/679 per conto di ciascun ente promotore per i trattamenti, diversi da quelli di cui al primo periodo del presente comma, necessari allo svolgimento delle attività ad essa affidate nell’ambito di ogni singola iniziativa” (art. 10, comma 2); il gestore è altresì titolare del trattamento con riferimento alla gestione dell’“anagrafica degli esercenti che supportano la piattaforma” (art. 10, comma 3);

gli issuer convenzionati “sono titolari del trattamento dei dati personali dei propri clienti”, mentre “agiscono in qualità di sub-responsabili del trattamento, individuati dal gestore della piattaforma in virtù di un’apposita convenzione, limitatamente allo svolgimento delle attività ad essi affidate ai sensi del presente decreto” (comma 4);

gli acquirer convenzionati “sono titolari del trattamento dei dati personali effettuato nell’ambito delle transazioni da essi gestite”, mentre “agiscono in qualità di sub-responsabili del trattamento, individuati dal gestore della piattaforma in virtù di un’apposita convenzione, limitatamente allo svolgimento delle attività ad essi affidate ai sensi del presente decreto” (art. 10, comma 4);

gli enti di supporto – cioè, i soggetti che hanno “in gestione una banca dati funzionale a verificare i dati richiesti dell’utente” (art. 1, comma 1, lett. k)) – “sono titolari del trattamento dei dati personali di cui alle rispettive banche dati, le quali possono essere interrogate, nell’ambito della gestione delle iniziative, al fine di verificare i dati degli utenti per l’adesione” (art. 10, comma 5);

il gestore della piattaforma è tenuto a predisporre la valutazione di impatto sulla protezione dei dati e a effettuare la consultazione preventiva ai sensi degli artt. 35 e 36 del Regolamento, ivi indicando, tra l’altro, le misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio, nonché a tutela dei diritti e delle libertà degli interessati, e disciplinando i tempi e le modalità di cancellazione dal programma (art. 10, comma 6);

ciascun ente promotore deve predisporre, laddove ne ricorrano i presupposti, la valutazione di impatto sulla protezione dei dati ed effettuare la consultazione preventiva per i trattamenti effettuati nell’ambito di ogni singola iniziativa (art. 10, comma 7);

il gestore, “previa anonimizzazione e aggregazione, può utilizzare i dati acquisiti per finalità di miglioramento dei servizi erogati, nonché per lo sviluppo della piattaforma e la valorizzazione del patrimonio aziendale” (art. 10, comma 9).

OSSERVA

Lo schema di decreto in esame, in attuazione dell’art. 28-bis del d.l. 152/2021, si occupa di disciplinare un complesso di trattamenti attraverso cui assicurare l’erogazione con modalità uniformi di benefici economici – destinati a specifici acquisti da effettuare attraverso terminali di pagamento fisici o virtuali ed erogati dalle pubbliche amministrazioni che aderiscono al progetto –

con l'obiettivo di digitalizzare i pagamenti della pubblica amministrazione e consentire un più efficiente controllo della spesa pubblica, semplificando l'accesso alle diverse iniziative da parte dei cittadini.

In particolare, per l'erogazione di tali benefici, viene previsto il ricorso a una nuova e distinta piattaforma, sempre gestita dalla società PagoPA, tramite cui sono raccolti ed elaborati dati relativi a operazioni di acquisto di beni o servizi.

I benefici possono erogati in due modalità. La prima comporta l'utilizzo dei c.d. "strumenti di pagamento" (come, ad esempio, le carte di pagamento), e prevede che, una volta acquisiti i dati necessari dall'acquirer in relazione ai pagamenti effettuati dagli utenti fruitori, l'ente erogatore disponga il rimborso sul conto corrente del beneficiario (previamente registrato dallo stesso sulla piattaforma). La seconda comporta, invece, l'utilizzo dei c.d. "strumenti di acquisto" (cioè strumenti in uso all'utente, che lo schema individua in SPID, CIE, App IO e tessera sanitaria), e prevede che, una volta identificato l'utente fruitore e verificata la spettanza del beneficio, questi vengano utilizzati dallo stesso per gli acquisti connessi alle iniziative degli enti promotori che dispongono il rimborso nei confronti dell'esercente per il tramite dell'acquirer.

3. Profili di criticità.

Preliminarmente si osserva che i trattamenti effettuati tramite la piattaforma in esame presentano rischi elevati per i diritti e le libertà degli interessati derivanti dalla raccolta massiva e generalizzata di informazioni di dettaglio, riferibili agli strumenti di pagamento (numero di carta di credito, ecc.) e ai conti correnti (IBAN) in uso agli utenti fruitori, nonché ad ogni aspetto della vita quotidiana dell'intera popolazione sulla base degli acquisti effettuati – classificabili anche in base all'identificativo fiscale dell'esercente e alla sua categoria merceologica o al codice categoria del prodotto acquistato e suscettibili di ricadere nell'ambito delle categorie particolari di dati personali –. Tali trattamenti di dati richiedono specifiche valutazioni in ordine alla proporzionalità del trattamento e all'individuazione delle misure da adottare al fine di rispettare i requisiti del Regolamento. La delicatezza del patrimonio informativo oggetto di trattamento, riguardante anche categorie di soggetti vulnerabili, richiede, infatti, l'adozione di rigorose misure tecniche e organizzative volte a mitigare i rischi di utilizzi impropri, oltre che di accessi non autorizzati, assicurando che tali dati siano trattati solo per le finalità di erogazione dei benefici richiesti.

Sebbene dall'esame schema di decreto non emergono tutti gli elementi, di dettaglio ma anche più generali, che sarebbero necessari a valutare adeguatamente la conformità del complesso dei trattamenti in esame al Regolamento e al Codice, si ritiene necessario evidenziare sin da ora i profili di criticità in ordine alla protezione dei dati personali, di seguito illustrati, relativi anche ad alcuni aspetti di competenza del Ministero dell'economia e delle finanze di cui non risulta ancora essere stato acquisito il concerto.

3.1. La raccolta dei dati relativi alle transazioni.

In primo luogo, si rileva che la piattaforma deve essere progettata, nel rispetto dei principi di minimizzazione dei dati e degli obblighi di protezione dei dati fin dalla progettazione e per impostazione predefinita (privacy by design e by default), limitando la raccolta dei dati a quelli strettamente necessari allo scopo perseguito, senza accentrare, presso PagoPA, i dati relativi a tutte le transazioni commerciali eseguite con gli strumenti di pagamento elettronici censiti dagli utenti, a prescindere dall'adesione alle diverse iniziative da parte degli interessati e dalla loro eleggibilità ai fini dell'erogazione dei benefici attraverso la piattaforma da parte degli enti promotori. Ciò, anche con particolare riferimento alla prospettata possibilità di acquisire dagli esercenti, attraverso gli acquirer, il codice categoria del bene o del servizio acquistato, che potrebbe comportare anche il trattamento di categorie particolari di dati personali, quali quelli relativi allo stato di salute degli interessati, per cui occorre prevedere l'adozione di garanzie

appropriate e specifiche in ogni fase del trattamento (artt. 9, par. 2, lett. g), del Regolamento e 2-sexies del Codice).

Pertanto, affinché la predetta raccolta dei dati relativi alle transazioni commerciali possa ritenersi proporzionata e conforme al Regolamento deve essere garantito che, per impostazione predefinita e fin dalla progettazione, gli esercenti, tramite gli acquirer, trasmettano a PagoPA esclusivamente i dati relativi a quelle transazioni di cui l'utente intende avvalersi per l'erogazione dei benefici economici connessi a iniziative a cui lo stesso ha aderito. Devono, pertanto, essere introdotte misure volte a escludere la trasmissione delle informazioni relative a transazioni che non risultino eleggibili a tal fine, limitando la raccolta alle sole informazioni di volta in volta necessarie in ragione delle caratteristiche delle singole iniziative (art. 25 del Regolamento).

Con particolare riferimento alla raccolta dei dati relativi al codice categoria dei beni acquistati, occorre poi prevedere l'introduzione di garanzie appropriate e specifiche in ogni fase del trattamento nel caso in cui da tale informazione possano emergere categorie particolari di dati personali.

3.2. Il trattamento dei dati relativi agli strumenti di pagamento e all'IBAN.

Lo schema di decreto prevede che l'utente possa registrare codici IBAN di conti correnti a lui intestati su cui ricevere i rimborsi previsti dalle diverse iniziative e che il gestore della piattaforma ne verifichi la titolarità in capo allo stesso utente (art. 6, commi 3 e 11). Non vengono invece previste misure per verificare l'intestazione all'utente degli strumenti di pagamento dallo stesso registrati nell'ambito della piattaforma.

Al riguardo, occorre osservare preliminarmente che la questione relativa alla titolarità dei conti correnti, ma anche degli strumenti di pagamento e di acquisto in capo all'utente che accede alla piattaforma, fa sorgere dubbi più generali sulle modalità con le quali si intende assicurare l'utilizzo della piattaforma proprio da parte di quelle particolari categorie di beneficiari – non in grado di avvalersene per impedimenti di diversa natura (disagio fisico, divario tecnologico, ecc.) – che potrebbero maggiormente giovarsi della semplificazione offerta da tale infrastruttura tecnologica per l'accesso alla pluralità di erogazioni offerte dalle pubbliche amministrazioni.

Dopo aver considerato le diverse ipotesi in cui il potenziale destinatario della misura potrebbe avere bisogno di avvalersi di un terzo per ottenere un beneficio economico attraverso la piattaforma e i connessi rischi per i diritti e le libertà degli interessati derivanti dall'esclusione dall'accesso a tale beneficio, è necessario, infatti, individuare misure a tal fine adeguate, tenendo anche in considerazione l'esigenza di prevenire frodi o abusi, realizzati mediante l'utilizzo di dati personali.

In tal senso, oltre ai controlli da effettuarsi sull'intestazione dei conti correnti, vanno altresì introdotti meccanismi con i quali si intende assicurare l'intestazione degli strumenti di pagamento – che possono essere utilizzati nell'ambito della piattaforma per ottenere i benefici – unicamente in capo agli utenti o ai beneficiari, individuando misure che consentano di escludere anche in tale contesto frodi o abusi, ovvero accessi non autorizzati, all'interno della piattaforma, ai dati personali relativi alle transazioni commerciali effettuate, nel rispetto del principio di riservatezza (art. 5, par. 1, lett. f), del Regolamento, analogamente a quando già osservato da Garante in relazione al c.d. Programma Cashback con il provvedimento n. 232 del 26 novembre 2020, disponibile in www.gpdp.it doc. web n. 9492345).

Pertanto, si ritiene necessario integrare lo schema di decreto prevedendo l'adozione di misure tecniche e organizzative per verificare la titolarità dei conti correnti e l'intestazione degli strumenti di pagamento, tenendo in considerazione anche i casi in cui gli utenti potrebbero operare sulla piattaforma in favore di terzi beneficiari, nel rispetto del principio di integrità e riservatezza e degli

obblighi di sicurezza (artt. 5, par. 1, lett. f), e 32 del Regolamento).

Più in generale, in relazione al trattamento dei dati relativi agli strumenti di pagamento, si rappresenta che il citato art. 28-bis prevede che, nell'erogazione dei benefici economici, ci si possa avvalere anche della piattaforma tecnologica di cui all'art. 5, comma 2, del CAD, gestita sempre da PagoPA. Tuttavia nello schema non emergono le attività di trattamento per quali è previsto l'utilizzo di quest'ultima piattaforma nell'ambito dell'erogazione dei benefici economici. Pertanto, si ritiene necessario che tali aspetti vengano precisati all'interno dello schema in esame.

In ogni caso, occorre precisare che il gestore della piattaforma può conservare i dati relativi agli strumenti di pagamento anche al fine di agevolare le operazioni di pagamento a favore di pubbliche amministrazioni da parte dell'utente tramite la piattaforma di cui all'art. 5, comma 2, del CAD, soltanto nel caso in cui acquisisca dallo stesso un consenso libero, specifico, informato, inequivocabile e facilmente revocabile, come evidenziato dalle "Raccomandazioni 02/2021 sulla base giuridica per la conservazione dei dati delle carte di credito al solo scopo di agevolare ulteriori operazioni online", adottate dal Comitato europeo per la protezione dei dati il 19 maggio 2021 (https://edpb.europa.eu/system/files/2021-07/recommendations022021_on_storage_of_credit_card_data_it.pdf).

3.3. L'utilizzo dei cc.dd. "strumenti di acquisto".

Dall'esame del testo dello schema in esame non risultano chiare le modalità con le quali si intendono utilizzare gli strumenti di acquisto, individuati in SPID, CIE, App IO, e tessera sanitaria (art. 1, comma 1, lett. x)), e il relativo PIN rilasciato mediante "i canali abilitanti gestiti dallo stesso gestore". In particolare, per i soli profili di competenza in materia di protezione dei dati personali, si rileva che non vengono chiarite le modalità di colloquio con i "dispositivi di accettazione" per la partecipazione alle iniziative, né quali strumenti possono essere utilizzati per acquisti effettuati online o fisicamente, che potrebbero richiedere l'individuazione di diverse misure per assicurare la conformità al Regolamento e al Codice di tali trattamenti.

Viene inoltre previsto che "il gestore della piattaforma, se l'utente registra uno strumento di acquisto, ottiene, mediante il codice fiscale fornito in sede di registrazione dallo stesso dall'Istituto Poligrafico e Zecca dello Stato S.p.A. i dati identificativi delle CIE e dall'Agenzia delle Entrate i dati identificativi della tessera sanitaria se non precedentemente disponibile all'interno dell'ecosistema di AppIO" (art. 6, comma 6).

Pur non essendo chiaro quali siano i "dati identificativi" della CIE e della tessera sanitaria a cui si fa riferimento, occorre, in ogni caso, rilevare che il titolare del trattamento dei dati relativi alla CIE non è l'IPZS ma il Ministero dell'interno (cfr. art. 62 del CAD e la relativa disciplina attuativa), mentre il titolare del trattamento di quelli relativi alla tessera sanitaria non è l'Agenzia delle entrate ma il Ministero dell'economia e delle finanze (cfr. art. 50 del d.l. 269/2003 e la relativa disciplina attuativa).
Sotto altro profilo, si osserva che lo schema di decreto prevede che la tessera sanitaria sia uno strumento identificativo dell'utente, al pari di SPID o CIE, e possa essere utilizzata quale specifico strumento di acquisto (cfr. artt. 1, comma 1, lett. x), e 8), pur non essendo tale strumento contemplato dal citato art. 28-bis del d.l. 152/2021, attuato dallo schema di decreto in esame; si rileva, infatti che l'art. 50, comma 1, del d.l. 30 settembre 2003, n. 269, stabilisce espressamente che la tessera sanitaria sia utilizzata "per potenziare il monitoraggio della spesa pubblica nel settore sanitario e delle iniziative per la realizzazione di misure di appropriatezza delle prescrizioni, nonché per l'attribuzione e la verifica del budget di distretto, di farmacovigilanza e sorveglianza epidemiologica".

In assenza di specifici chiarimenti sulle modalità di utilizzo dei citati strumenti di acquisto, che richiedono anche approfondimenti sulla compatibilità dell'utilizzo della tessera sanitaria nel

generico contesto dell'erogazione di benefici economici, senza indicazione delle misure che si intendono adottare al fine di rispettare i principi di "liceità, correttezza e trasparenza", di "limitazione della finalità" e di "integrità e riservatezza" di cui all'art. 5, par. 1, lett. a), b) e f), del Regolamento, non è possibile valutare adeguatamente i predetti aspetti in relazione al trattamento dei dati personali correlato.

Occorre pertanto integrare lo schema di decreto precisando quali siano i "dati identificativi" della CIE e della tessera sanitaria che si intende utilizzare e individuando correttamente i titolari del trattamento presso cui si intendono acquisire tali informazioni. Inoltre, deve essere valutato accuratamente l'impiego della tessera sanitaria in tale contesto nel rispetto di quanto previsto dal citato art. 50 del d.l. n. 269/2003 e dalla normativa di settore.

In ogni caso, la conformità dell'utilizzo degli strumenti di acquisto nell'ambito della piattaforma dovrà essere valutata da parte di questa Autorità una volta acquisiti ulteriori elementi anche nell'ambito dell'esame della valutazione di impatto predisposta dal gestore della piattaforma (art. 35 del Regolamento), tenendo conto delle indicazioni che potranno essere fornite al riguardo dal Ministero dell'interno (per la CIE) e dal Ministero dell'economia e delle finanze (per la tessera sanitaria).

3.4. La sicurezza dei trattamenti e la conservazione dei dati.

Lo schema di decreto prevede che "il gestore della piattaforma cura la manutenzione della stessa al fine di garantire il rispetto ogni standard tecnologico in materia di sicurezza e di tutela dei dati personali e provvede al suo aggiornamento tecnologico, nonché alla divulgazione delle sue specifiche tecniche agli acquirer convenzionati, agli issuer convenzionati e agli enti promotori e, in ogni caso, a tutti i soggetti coinvolti nell'erogazione del servizio" (art. 3, comma 8) e che "il gestore della piattaforma deve predisporre la valutazione di impatto ai sensi dell'articolo 35 del regolamento UE 2016/679 ed effettuare la consultazione preventiva ai sensi dell'articolo 36. Nella valutazione di impatto sono indicate, tra l'altro, le misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio, nonché a tutela dei diritti e delle libertà degli interessati" (art. 10, comma 6).

Al riguardo, si osserva che le caratteristiche dei trattamenti disciplinati dallo schema in esame richiedono l'adozione di idonee misure tecniche e organizzative volte a garantire un livello di sicurezza adeguato ai rischi elevati, sopra evidenziati, riferibili alle diverse attività poste in essere dai soggetti a vario titolo coinvolti nell'erogazione dei benefici attraverso la piattaforma (gestore, acquirer, issuer, esercenti, enti promotori ed enti di supporto).

Lo schema di decreto individua infatti diversi "canali abilitanti" (come l'App IO, altri canali offerti dal gestore o canali fisici o digitali messi a disposizione dagli issuer convenzionati) per consentire all'utente di accedere alla piattaforma e utilizzare i servizi ivi resi disponibili (cfr. art. 1, comma 1, lett. e), e, in particolare, artt. 6 e 8).

Al fine di prevenire i rischi di accessi abusivi o illeciti alla piattaforma, occorre quindi assicurare che i diversi canali di accesso siano dotati di garanzie uniformi, predisposte dal gestore e dagli altri soggetti coinvolti (es. issuer) nel rispetto dei principi di integrità e riservatezza e di privacy by design e by default e degli obblighi di sicurezza (art. 5, par. 1, lett. f), e artt. 24, 25 e 32 del Regolamento).

Pertanto, si ritiene necessario che lo schema di decreto sia integrato prevedendo che sia garantita un'adeguata protezione dei dati in ogni fase dei trattamenti e in relazione a ogni canale di accesso alla piattaforma, attraverso l'adozione di misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio, con particolare riferimento alle informazioni relativi agli strumenti di pagamento e alle transazioni commerciali, al fine di assicurare che siano trattate solo

per le finalità di erogazione dei benefici e non siano oggetto di utilizzi impropri o accessi non autorizzati.

Con riferimento invece al principio di limitazione della conservazione (art. 5, par. 1, lett. e), del Regolamento), si rileva che nello schema in esame non vengono, tuttavia, individuate, misure che garantiscano l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle specifiche finalità del trattamento, cancellando tempestivamente i dati non più necessari, neanche attraverso il rinvio a un ulteriore atto attuativo.

Si ritiene pertanto necessario che, nello schema, anche eventualmente attraverso il rinvio a un successivo atto attuativo, siano individuati i tempi di conservazione che dovrebbero essere differenziati in ragione delle diverse tipologie di dati e delle finalità per le quali sono trattati.

Sotto altro aspetto, lo schema demanda alla valutazione di impatto l'individuazione dei "tempi e le modalità di cancellazione dal programma" (art. 10, comma 6, riferibile più correttamente alle singole iniziative o, più in generale, alla piattaforma), che non risulta del tutto allineato con l'art. 6, comma 12, che prevede che "la cancellazione dall'iniziativa determina sia la perdita del diritto a concorrere all'assegnazione del beneficio secondo le regole dell'iniziativa fissate dall'ente promotore, sia la cancellazione di tutti i dati personali inerenti l'utente fruitore con riferimento alla singola iniziativa, fatta salva l'ipotesi in cui sussistano ulteriori basi giuridiche del trattamento, ivi inclusa quella di fare fronte a eventuali contestazioni o contenziosi".

Al riguardo, si osserva che "la cancellazione dall'iniziativa" da parte di un utente, a seconda delle caratteristiche della stessa, potrebbe non richiedere, per impostazione predefinita, "la cancellazione di tutti i dati personali inerenti l'utente fruitore con riferimento alla singola iniziativa", soprattutto con riferimento a benefici già erogati attraverso la piattaforma, i cui dati non sarebbero più a sua disposizione.

Occorre, pertanto, integrare lo schema prevedendo che anche gli utenti che abbiano richiesto la cancellazione dalle singole iniziative possano consultare i dati fino a quel momento raccolti, disciplinando i tempi di conservazione degli stessi ai sensi di quanto sopra rappresentato, tenendo conto delle caratteristiche delle singole iniziative e nel rispetto del principio di limitazione della conservazione.

3.5. Altri aspetti.

3.5.1. Lo schema di decreto definisce "enti promotori" le amministrazioni che erogano i benefici previsti attraverso la piattaforma, peraltro includendo espressamente la Ragioneria generale dello Stato per le iniziative di sua competenza (cfr. art. 1, comma 1, lett. l)).

Al riguardo, si osserva che l'ordinamento definisce i soggetti che erogano prestazioni sociali quali "enti erogatori", attribuendo puntuali competenze, anche relative al trattamento di dati personali, nell'ambito della disciplina in materia di ISEE (cfr. spec. d.P.C.M. 5 dicembre 2013, n. 159). Non risulta chiara, in tale prospettiva, l'assimilazione a tali soggetti della Ragioneria generale dello Stato, con un ruolo distinto da questi ultimi, prospettando, peraltro, l'assunzione da parte della stessa del ruolo di titolare del trattamento, in luogo del Ministero dell'economia e delle finanze.

Pertanto, si ritiene necessario chiarire il riferimento alla Ragioneria generale dello Stato nell'ambito degli "enti promotori" contenuto nello schema di decreto (art. 1, comma 1, lett. l)).

3.5.2. Lo schema di decreto definisce l'App IO, canale di accesso alla piattaforma, come Punto di accesso telematico ai sensi dell'art. 64-bis del CAD (cfr. art. 1, comma 1, lett. b)).

Sul punto si osserva che, in base alle "Linee guida sul punto di accesso telematico ai servizi della Pubblica Amministrazione" (adottate dall'AgiD con determinazione n. 598 dell'8 novembre 2021),

l'App IO costituisce solo una delle componenti del Punto di accesso telematico di cui all'art. 64-bis del CAD, poiché è previsto che lo stesso sia altresì costituito da un'interfaccia versione web (cfr. parr. 2.5 e 3.2 delle citate Linee guida).

Pertanto, nel rispetto del principio di liceità, correttezza e trasparenza (art. 5, par. 1, lett. a), del Regolamento), si ritiene necessario che ogni riferimento all'"App IO" contenuto nello schema di decreto sia sostituito dal riferimento al "Punto di accesso telematico".

Sotto altro aspetto, in relazione al prospettato invio agli "utenti di app IO o di altri canali nella titolarità del gestore della piattaforma", da parte della piattaforma, di "ogni informazione utile in merito alle iniziative mediante servizi di messaggistica" (art. 6, comma 13), si ritiene necessario richiamare quanto previsto dalle citate Linee guida che stabiliscono che "Il Gestore deve consentire all'utente un meccanismo di opt-in per l'attivazione dei servizi disponibili nel Punto di accesso telematico, garantendo a tutti gli interessati una scelta libera, esplicita e specifica" (cap. 4), in analogia al servizio "Novità e aggiornamenti" dell'App IO tramite il quale PagoPA fornisce, su richiesta degli utenti, aggiornamenti anche in relazione ai nuovi servizi resi disponibili.

3.5.3. Lo schema di decreto prevede che l'accesso alla piattaforma avvenga previa autenticazione con SPID o CIE, di livello di sicurezza almeno significativo (art. 1, comma 1, lett. e) e x)), sia da parte degli utenti (cfr. spec. art. 6, comma 1) che da parte degli operatori delle amministrazioni erogatrici (cfr. spec. artt. 4, 5, comma 1).

Tuttavia, l'art. 64, comma 2-nonies, del CAD prevede che l'accesso ai servizi in rete erogati dalle pubbliche amministrazioni che richiedono il superamento di una procedura di autenticazione informatica possa avvenire anche con la Carta nazionale dei servizi (di seguito "CNS"), laddove il canale abilitante sia compatibile con l'utilizzo di tale strumento.

Pertanto, al fine di assicurare pari condizioni di accesso ad una più ampia platea di potenziali beneficiari, nel rispetto del principio di liceità, correttezza e trasparenza (art. 5, par. 1, lett. a), del Regolamento), si ritiene opportuno integrare lo schema di decreto introducendo la possibilità di accedere alla piattaforma autenticandosi anche mediante CNS, laddove il canale abilitante sia compatibile con l'utilizzo di tale strumento.

3.5.4. In tema di verifiche sul possesso dei requisiti necessari alla fruizione di un beneficio da parte di un utente, lo schema di decreto, tra le varie modalità, prevede anche la collaborazione con i soggetti che hanno in gestione le banche dati recanti le informazioni necessarie per la suddetta verifica (art. 6, comma 8). Anche per le verifiche che riguardano il legale rappresentante di una persona giuridica beneficiaria – in relazione alle quali l'art. 6, comma 7, richiama il Registro delle imprese (per le imprese) e le basi dati dell'Agenzia delle entrate (per ogni altro soggetto pubblico o privato non tenuto all'iscrizione nel Registro delle imprese) – viene previsto che il gestore possa "integrarsi con ogni ente in grado di fornirgli supporto nonché […] accedere alle informazioni dell'utente disponibili nelle relative banche dati" (cfr. art. 6, comma 9). Infatti, viene definito "ente di supporto" quel soggetto che abbia in "gestione" una banca dati funzionale a verificare i dati richiesti dell'utente (cfr. art. 1, comma 1, lett. k)).
In proposito si rileva che le verifiche in questione devono essere effettuate, laddove previsto nell'ambito della base giuridica che disciplina l'erogazione dei benefici da parte dell'ente erogatore, con riferimento alle sole informazioni necessarie e utilizzando le pertinenti banche dati, nel rispetto di quanto previsto dalle norme di settore e dei principi di liceità, correttezza e trasparenza, di minimizzazione dei dati, di esattezza e di integrità e riservatezza (art. 5, par. 1, lett. a), c), d) e f), del Regolamento).

Non risulta inoltre precisato il ruolo assunto dal gestore della piattaforma nell'ambito dei trattamenti di dati personali effettuati, per conto degli enti promotori, ai fini delle citate verifiche, con particolare riferimento a quelle di cui agli artt. 6, comma 8, e 8, comma 4.

Pertanto, si ritiene necessario che lo schema di decreto sia integrato precisando il ruolo assunto dal gestore della piattaforma nell'ambito delle verifiche, nonché specificando puntualmente le tipologie di dati personali oggetto delle verifiche in questione, le banche dati a tal fine utilizzate e i relativi titolari del trattamento, ovvero, laddove ciò non sia possibile, precisando che tali verifiche dovranno avvenire sulla base della normativa di settore che disciplina l'erogazione del beneficio, adottando misure adeguate a rispettare i principi di liceità, correttezza e trasparenza, di minimizzazione dei dati, di esattezza e di integrità e riservatezza (art. 5, par. 1, lett. a), c), d) e f), del Regolamento).

3.5.5. Lo schema di decreto, in attuazione del comma 5 dell'art. 28-bis del d.l. 152/2021, prevede la comunicazione di alcuni flussi contabili relativi ai benefici dal gestore della piattaforma al Ministero dell'economia e delle finanze, da definire mediante apposita convenzione, ma non risulta chiaro se, in tale contesto, sono trasmessi anche dati personali.

Pertanto, nel rispetto dei principi di liceità, correttezza e trasparenza, di minimizzazione dei dati e di privacy by design e by default (artt. 5, par. 1, lett. a) e c), e 25 del Regolamento), occorre valutare la necessità di includere dati personali nei predetti flussi contabili e, se del caso, individuando i dati personali che devono essere necessariamente oggetto di comunicazione, limitandoli a quelli pertinenti e non eccedenti al perseguimento delle finalità previste dall'art. 28-bis, comma 5, del d.l. 152/2021.

3.5.6. Lo schema di decreto prevede che "il gestore della piattaforma detiene un'anagrafica degli esercenti che supportano la piattaforma e, al fine della corretta gestione della stessa, tratta i relativi dati personali in qualità di titolare del trattamento" (art. 10, comma 3).

Il ruolo assunto dagli esercenti nei trattamenti dei dati personali necessari per l'erogazione dei benefici economici emerge, in particolare, in più punti dello schema sia in relazione all'integrazione dei propri sistemi con quelli dell'acquirer per la trasmissione alla piattaforma dei dati relativi alle transazioni commerciali, che per i rimborsi ad essi spettanti in caso di benefici erogati tramite strumenti di acquisto (artt. 7, 8 e 9).

Al riguardo, si osserva che non sono chiare le modalità di adesione degli esercenti alla piattaforma, non sono indicate le tipologie di dati personali che gli esercenti devono conferire a tal fine, contenuti nella predetta "anagrafica", né quali di questi dati (che potrebbero riguardare anche esercenti persone fisiche) potrebbe essere necessario rendere disponibili agli utenti fruitori al fine di agevolare la fruizione dei benefici.

Pertanto, fermo restando quanto indicato in relazione alla sicurezza dei trattamenti – riferibili anche alle integrazioni tra i sistemi degli esercenti e degli acquirer e, più in generale, alle loro interazioni con la piattaforma – occorre che siano individuate le modalità di adesione degli esercenti alla piattaforma, le tipologie di dati personali che gli stessi devono conferire a tal fine e quelli che potrebbe essere necessario rendere disponibili agli utenti fruitori, mediante comunicazione o diffusione (artt. 5, par. 1, lett. a), e 6, par. 3, del Regolamento e art. 2-ter del Codice).

RITENUTO

Alla luce di quanto sopra osservato, al fine di assicurare la conformità al Regolamento e al Codice in relazione ai trattamenti di dati personali effettuati nell'ambito della piattaforma per l'erogazione di benefici economici, che presentano rischi elevati per i diritti e le libertà fondamentali degli interessati, si ritiene necessario che lo schema di decreto in esame debba essere modificato e integrato sulla base delle condizioni, descritte e motivate nel paragrafo 3.

Inoltre, nel ribadire, come rilevato in motivazione, che nello schema di decreto non sono indicati

alcuni elementi necessari a consentire la verifica del pieno rispetto della normativa in materia di protezione dei dati personali nell'ambito del complesso dei trattamenti che verranno posti in essere in attuazione del citato art. 28-bis del d.l. 152/2021, questa Autorità si riserva di analizzare tali aspetti anche nell'ambito dell'esame della valutazione di impatto sulla protezione dei dati che verrà svolta dal gestore della piattaforma ai sensi degli artt. 35 e 36, par. 5, del Regolamento (art. 10, comma 6), anche in considerazione dei rischi elevati che non risultano essere mitigati adeguatamente dalle misure allo stato individuate.

TUTTO CIÒ PREMESSO, IL GARANTE

ai sensi degli artt. 36, par. 4, e 58, par. 3, lett. b), del Regolamento, esprime, nei termini di cui in motivazione, il richiesto parere sullo schema di decreto del Ministro per l'innovazione tecnologica e la transizione digitale in materia di piattaforma digitale per l'erogazione di benefici economici concessi dalle amministrazioni pubbliche, da adottare, di concerto con il Ministro dell'economia e delle finanze, ai sensi dell'art. 28-bis, comma 3, del d.l. 6 novembre 2021, n. 152, convertito, con modificazioni, dalla l. 29 dicembre 2021, n. 233, a condizione che lo schema sia modificato e integrato prevedendo che:

a) gli esercenti, tramite gli acquirer, trasmettano a PagoPA, per impostazione predefinita e fin dalla progettazione, esclusivamente i dati relativi a quelle di cui l'utente intende avvalersi per l'erogazione dei benefici economici connessi a iniziative a cui lo stesso ha aderito, introducendo misure volte a escludere la trasmissione delle informazioni relative a transazioni che non risultino eleggibili a tal fine, limitando la raccolta alle sole informazioni di volta in volta necessarie in ragione delle caratteristiche delle singole iniziative (cfr. par. 3.1);

b) con riferimento alla raccolta dei dati relativi al codice categoria dei beni acquistati, siano introdotte garanzie appropriate e specifiche in ogni fase del trattamento (cfr. par. 3.1);

c) siano adottate misure tecniche e organizzative per verificare la titolarità dei conti correnti e l'intestazione degli strumenti di pagamento, tenendo in considerazione anche i casi in cui gli utenti potrebbero operare sulla piattaforma in favore di terzi beneficiari (cfr. par. 3.2);

d) siano precisate le attività di trattamento effettuate mediante l'utilizzo della piattaforma di cui all'art. 5, comma 2, del CAD, al fine dell'erogazione dei benefici (cfr. par. 3.2);

e) siano precisati i "dati identificativi" della CIE e della tessera sanitaria necessari per consentirne l'utilizzo quali strumenti di acquisto e siano individuati correttamente i titolari del trattamento presso cui si intendono acquisire tali informazioni, valutando accuratamente l'impiego della tessera sanitaria in tale contesto, anche alla luce delle indicazioni che potranno essere fornite al riguardo dal Ministero dell'interno e dal Ministero dell'economia e delle finanze (cfr. par. 3.3);

f) sia assicurata un'adeguata protezione dei dati in ogni fase dei trattamenti e in relazione a ogni canale di accesso alla piattaforma, attraverso l'adozione di misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio, con particolare riferimento alle informazioni relativi agli strumenti di pagamento e alle transazioni commerciali (cfr. par. 3.4);

g) siano disciplinati i tempi di conservazione dei dati trattati nell'ambito della piattaforma e sia assicurato che anche gli utenti che abbiano richiesto la cancellazione

dalle singole iniziative possano consultare i dati fino a quel momento raccolti (cfr. par. 3.4);

h) sia precisato il riferimento alla Ragioneria generale dello Stato nell'ambito degli "enti promotori" (cfr. par. 3.5.1) e sia indicato il riferimento al "Punto di accesso telematico" in luogo dell'"App IO" (cfr. par. 3.5.2);

i) sia precisato il ruolo assunto dal gestore della piattaforma nell'ambito delle verifiche e siano indicate le tipologie di dati personali oggetto delle stesse, le banche dati a tal fine utilizzate, ovvero, laddove ciò non sia possibile, sia stabilito che tali verifiche dovranno avvenire sulla base della normativa di settore che disciplina l'erogazione del beneficio (cfr. par. 3.5.4);

l) sia valutata la necessità di includere dati personali nei flussi contabili relativi ai benefici e, se del caso, siano individuati i dati personali che devono essere necessariamente oggetto di comunicazione al Ministero dell'economia e delle finanze - Ragioneria generale dello Stato (cfr. par. 3.5.5);

m) siano individuate le modalità di adesione degli esercenti alla piattaforma, le tipologie di dati personali che gli stessi devono conferire a tal fine e quelli oggetto di eventuale comunicazione o diffusione (cfr. par. 3.5.6);

e con la seguente osservazione:

n) sia introdotta la possibilità di accedere alla piattaforma autenticandosi anche mediante CNS, laddove il canale abilitante sia compatibile con l'utilizzo di tale strumento (cfr. par. 3.5.3).

L'Autorità si riserva, inoltre, di analizzare gli elementi non indicati nello schema di decreto, necessari alla verifica del pieno rispetto della normativa in materia di protezione dei dati personali, nell'ambito dell'esame della valutazione di impatto sulla protezione dei dati che verrà svolta dal gestore della piattaforma ai sensi degli artt. 35 e 36, par. 5, del Regolamento, anche in considerazione dei rischi elevati che non risultano essere mitigati adeguatamente dalle misure allo stato individuate.

Roma, 28 luglio 2022

IL PRESIDENTE
Stanzione

IL RELATORE
Scorza

IL SEGRETARIO GENERALE
Mattei