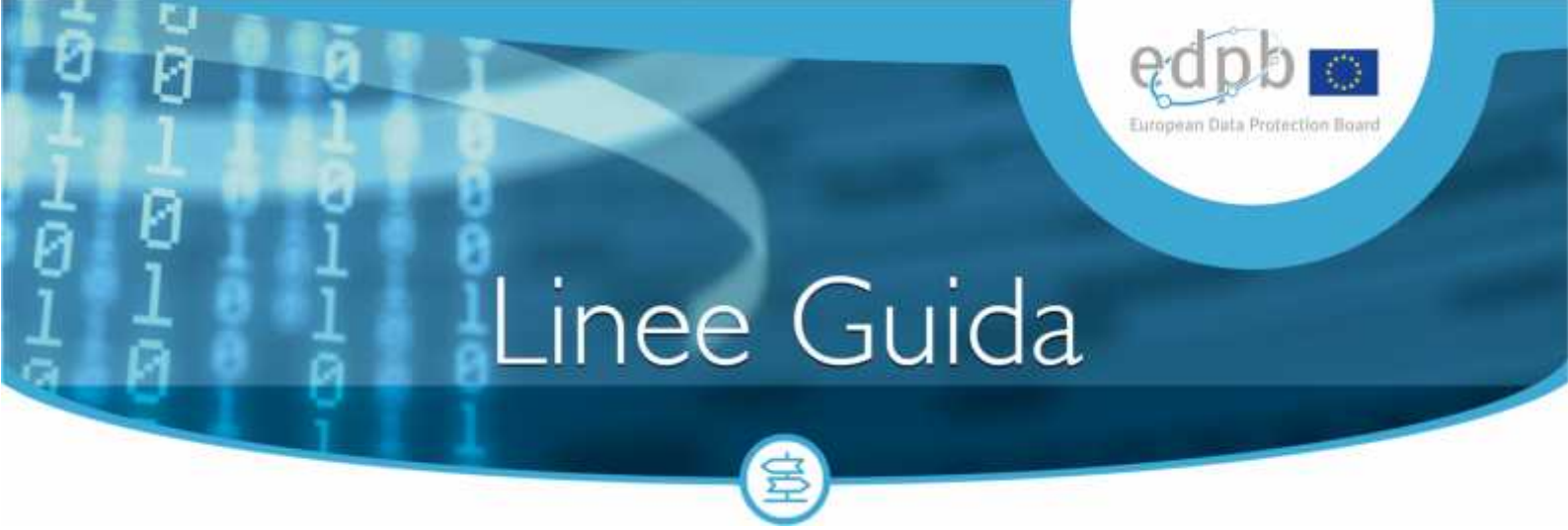

Linee guida 06/2020 sull'interazione tra la seconda direttiva sui servizi di pagamento e il GDPR

Versione 2.0

Adottate il 15 dicembre 2020

Cronologia delle versioni

Versione 2.0	15.12.2020	Adozione delle linee guida a seguito della consultazione pubblica
Versione 1.0	17.07.2020	Adozione delle linee guida ai fini della consultazione per la pubblicazione

Indice

Il Comitato europeo per la protezione dei dati,

visto l'articolo 70, paragrafo 1, lettera e), 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),

visto l'accordo sullo Spazio economico europeo (SEE), in particolare l'allegato XI e il protocollo 37, modificati dalla decisione del comitato misto SEE n. 154/2018 del 6 luglio 2018[1],

visti gli articoli 12 e 22 del proprio regolamento interno,

considerando quanto segue:

(1) Il regolamento generale sulla protezione dei dati (di seguito "GDPR") prevede un insieme coerente di norme per il trattamento dei dati personali in tutta l'UE.

(2) La seconda direttiva sui servizi di pagamento (direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio, del 25 dicembre 2015, di seguito "PSD2") abroga la direttiva 2007/64/CE e stabilisce nuove norme per garantire certezza giuridica ai consumatori, ai commercianti e alle imprese nella catena di pagamento e per modernizzare il quadro giuridico riguardante il mercato dei servizi di pagamento[2]. Gli Stati membri erano tenuti a recepire la PSD2 nei rispettivi ordinamenti nazionali entro il 13 gennaio 2018.

(3) Un elemento importante della PSD2 è l'introduzione di un quadro giuridico per i nuovi servizi di disposizione di ordine di pagamento e servizi di informazione sui conti. La PSD2 consente ai prestatori di questi nuovi servizi di pagamento di avere accesso ai conti di pagamento degli interessati ai fini della prestazione di detti servizi.

(4) Per quanto riguarda la protezione dei dati, a norma dell'articolo 94, paragrafo 1, della PSD2, qualsiasi trattamento di dati personali, compresa la fornitura di informazioni in merito al trattamento, ai fini della PSD2 deve essere effettuato in conformità del GDPR[3] e del regolamento (UE) 2018/1725.

(5) Il considerando 89 della PSD2 afferma che, qualora ai fini della direttiva vi sia trattamento di dati personali, è opportuno che sia specificato lo scopo preciso, siano citate le basi giuridiche pertinenti, vi sia conformità con i requisiti di sicurezza pertinenti di cui al GDPR e siano rispettati i principi di necessità, proporzionalità, limitazione delle finalità e proporzionalità del periodo di conservazione dei dati. Inoltre la protezione dei dati fin dalla progettazione e la protezione dei dati per impostazione predefinita dovrebbero essere integrate in tutti i sistemi di trattamento dei dati sviluppati e utilizzati nel quadro della PSD2[4].

(6) Il considerando 93 della PSD2 afferma che i prestatori di servizi di disposizione di ordine di pagamento e i prestatori di servizi di informazione sui conti, da una parte, e il prestatore di servizi di pagamento di radicamento del conto, dall'altra, dovrebbero soddisfare i necessari requisiti in materia

[1] Nel presente documento, i riferimenti agli "Stati membri" sono da intendersi come riferimenti agli "Stati membri del SEE".

[2] Considerando 6 della PSD2.

[3] Poiché la PSD2 è precedente al GDPR, fa ancora riferimento alla direttiva 95/46/CE. L'articolo 94 del GDPR stabilisce che i riferimenti alla direttiva 95/46/CE abrogata si intendono fatti al GDPR.

[4] Considerando 89 della PSD2.

di protezione e sicurezza dei dati stabiliti o citati nella direttiva o indicati nei progetti di norme tecniche di regolamentazione,

HA ADOTTATO LE SEGUENTI LINEE GUIDA:

1. INTRODUZIONE

1. La seconda direttiva sui servizi di pagamento (di seguito "PSD2") ha introdotto una serie di novità nel settore dei servizi di pagamento. Pur creando nuove opportunità per i consumatori e aumentando la trasparenza in tale ambito, l'applicazione della PSD2 solleva alcune questioni e preoccupazioni riguardo alla necessità che gli interessati mantengano il pieno controllo dei loro dati personali. Il regolamento generale sulla protezione dei dati (di seguito "GDPR") si applica al trattamento dei dati personali, comprese le attività di trattamento effettuate nell'ambito di servizi di pagamento ai sensi della PSD2[5]. Pertanto i titolari del trattamento che operano nel settore disciplinato dalla PSD2 devono sempre garantire il rispetto dei requisiti del GDPR, compresi i principi di protezione dei dati di cui all'articolo 5 dello stesso, e delle pertinenti disposizioni della direttiva relativa alla vita privata e alle comunicazioni elettroniche[6]. Benché la PSD2[7] e le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri (di seguito "norme tecniche di regolamentazione"[8]) contengano talune disposizioni relative alla protezione e alla sicurezza dei dati, sono emerse incertezze circa l'interpretazione di tali disposizioni e l'interazione tra il quadro generale in materia di protezione dei dati e la PSD2.

2. Il 5 luglio 2018 l'EDPB ha pubblicato una lettera relativa alla PSD2, nella quale ha fornito chiarimenti su questioni relative alla protezione dei dati personali in relazione alla PSD2, in particolare sul trattamento dei dati personali di soggetti diversi dai contraenti (i cosiddetti "*silent party data*", ossia i "dati dei taciti interessati") da parte dei prestatori di servizi di informazione sui conti (di seguito "AISP") e dei prestatori di servizi di disposizione di ordine di pagamento (di seguito "PISP"), sulle procedure relative alla prestazione e alla revoca del consenso, sulle norme tecniche di regolamentazione e sulla cooperazione tra i prestatori di servizi di pagamento di radicamento del conto (di seguito "ASPSP") in relazione alle misure di sicurezza. Al fine di individuare le sfide più urgenti da affrontare, nell'ambito dell'attività di formulazione delle presenti linee guida si è provveduto a raccogliere contributi delle parti interessate, sia per iscritto che in occasione di un evento dedicato ai portatori di interessi.

3. L'obiettivo delle presenti linee guida è fornire ulteriori orientamenti su aspetti relativi alla protezione dei dati nel contesto della PSD2, in particolare sulla relazione tra le pertinenti

---

5 Articolo 1, paragrafo 1, del GDPR.

6 Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche). (GU L 201 del 31.7.2002, pag. 37).

7 Articolo 94 della direttiva sui servizi di pagamento, ecc.

8 Regolamento delegato (UE) 2018/389 della Commissione, del 27 novembre 2017, che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri (Testo rilevante ai fini del SEE), C/2017/7782 (GU L 69 del 13.3.2018, pag. 23) consultabile all'indirizzo https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32018R0389&from=IT.

disposizioni del GDPR e della direttiva. Le presenti linee guida si concentrano principalmente sul trattamento dei dati personali da parte degli AISP e dei PISP. Di conseguenza il presente documento verte sulle condizioni necessarie affinché gli ASPSP possano concedere l'accesso alle informazioni sui conti di pagamento e affinché i PISP e gli AISP possano procedere al trattamento dei dati personali, compresi i requisiti e le garanzie vigenti in relazione al trattamento dei dati personali da parte dei PISP e degli AISP per fini diversi dalle finalità iniziali per le quali i dati sono stati raccolti, in particolare nel caso in cui siano stati raccolti nell'ambito della prestazione di un servizio di informazione sui conti[9]. Nel presente documento vengono discusse inoltre le diverse nozioni di consenso esplicito ai sensi della PSD2 e del GDPR, nonché il trattamento dei "dati dei taciti interessati", il trattamento di categorie particolari di dati personali da parte dei PISP e degli AISP, l'applicazione dei principi fondamentali di protezione dei dati stabiliti dal GDPR, tra cui la minimizzazione dei dati, la trasparenza, la responsabilizzazione e le misure di sicurezza. La PSD2 comporta responsabilità trasversali nei settori, tra l'altro, della protezione dei consumatori e del diritto in materia di concorrenza. Le considerazioni relative a tali ambiti del diritto esulano dall'oggetto delle presenti linee guida.

4. Per agevolare la lettura delle linee guida, si riportano di seguito le definizioni dei principali termini utilizzati nel presente documento.

1.1 Definizioni

"Prestatore di servizi di informazione sui conti" ("AISP"): il prestatore di un servizio online che fornisce informazioni consolidate relativamente a uno o più conti di pagamento detenuti dall'utente di servizi di pagamento presso un altro prestatore di servizi di pagamento o presso più prestatori di servizi di pagamento.

"Prestatore di servizi di pagamento di radicamento del conto" ("ASPSP"): un prestatore di servizi di pagamento che fornisce e amministra un conto di pagamento per un pagatore.

"Minimizzazione dei dati": un principio di protezione dei dati in base al quale i dati personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

"Pagatore": una persona fisica o giuridica detentrice di un conto di pagamento che autorizza l'ordine di pagamento a partire da detto conto di pagamento o, in mancanza di conto di pagamento, una persona fisica o giuridica che dà l'ordine di pagamento.

"Beneficiario": una persona fisica o giuridica che è il destinatario previsto dei fondi che sono stati oggetto di un'operazione di pagamento.

"Conto di pagamento": un conto detenuto a nome di uno o più utilizzatori di servizi di pagamento utilizzato per l'esecuzione di operazioni di pagamento.

"Prestatore di servizi di disposizione di ordine di pagamento" ("PISP"): il prestatore di un servizio che dispone l'ordine di pagamento su richiesta dell'utente di servizi di pagamento relativamente a un conto di pagamento detenuto presso un altro prestatore di servizi di pagamento.

[9] Un servizio di informazione sui conti è un servizio online che fornisce informazioni consolidate relativamente a uno o più conti di pagamento detenuti dall'utente di servizi di pagamento presso un altro prestatore di servizi di pagamento o presso più prestatori di servizi di pagamento.

"Prestatore di servizi di pagamento": un organismo di cui all'articolo 1, paragrafo 1, della PSD2[10] o una persona fisica o giuridica che beneficia di un'esenzione ai sensi dell'articolo 32 o 33 della PSD2.

"Utente di servizi di pagamento": persona fisica o giuridica che si avvale di un servizio di pagamento in qualità di pagatore, di beneficiario o di entrambi.

"Dato personale": qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

"Protezione dei dati fin dalla progettazione": misure tecniche e organizzative, integrate in un prodotto o servizio, volte ad attuare in modo efficace i principi di protezione dei dati e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del GDPR e tutelare i diritti degli interessati.

"Protezione dei dati per impostazione predefinita": adeguate misure tecniche e organizzative, integrate in un prodotto o servizio, che garantiscono che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.

"Nome tecniche di regolamentazione": il regolamento delegato (UE) 2018/389 della Commissione, del 27 novembre 2017, che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri.

"Prestatori terzi": sia i PISP che gli AISP.

1.2 Servizi nell'ambito della PSD2

5. La PSD2 introduce due nuovi tipi di (prestatori di) servizi di pagamento: i PISP e gli AISP. Nell'allegato I della PSD2 figurano gli otto servizi di pagamento disciplinati dalla stessa.

6. I "PISP" prestano servizi che dispongono ordini di pagamento su richiesta dell'utente di servizi di pagamento relativamente a un conto di pagamento dell'utente detenuto presso un altro prestatore di servizi di pagamento[11]. Un PISP può richiedere a un ASPSP (generalmente una banca)

---

[10] L'articolo 1, paragrafo 1, della PSD2 afferma che la direttiva stabilisce le regole in base alle quali gli Stati membri devono distinguere le seguenti categorie di *prestatori di servizi di pagamento*:
a) gli enti creditizi quali definiti all'articolo 4, paragrafo 1, punto 1), del regolamento (UE) n. 575/2013 del Parlamento europeo e del Consiglio (1), comprese le relative succursali quali definite al relativo punto 17), se tali succursali sono situate nell'Unione, indipendentemente dal fatto che le sedi centrali di dette succursali siano situate nell'Unione ovvero, conformemente all'articolo 47 della direttiva 2013/36/UE e alla normativa nazionale, al di fuori dell'Unione;
b) gli istituti di moneta elettronica quali definiti all'articolo 2, punto 1), della direttiva 2009/110/CE, comprese – conformemente all'articolo 8 di detta direttiva e al diritto nazionale – le relative succursali qualora queste siano situate nell'Unione e le loro sedi centrali siano situate al di fuori dell'Unione, nella misura in cui i servizi di pagamento prestati da dette succursali siano connessi all'emissione di moneta elettronica;
c) gli uffici postali che hanno il diritto di prestare servizi di pagamento a norma del diritto nazionale;
d) gli istituti di pagamento;
e) la BCE e le banche centrali nazionali ove non agiscano in quanto autorità monetarie o altre autorità pubbliche;
f) gli Stati membri o le rispettive autorità regionali o locali ove non agiscano in quanto autorità pubbliche.

[11] Articolo 4, punto 15), della PSD2.

di disporre un'operazione per conto dell'utente di servizi di pagamento. L'utente (di servizi di pagamento) può essere una persona fisica (interessato) o una persona giuridica.

7. Gli AISP prestano servizi online che forniscono informazioni consolidate relativamente a uno o più conti di pagamento detenuti dall'utente di servizi di pagamento presso un altro prestatore di servizi di pagamento o presso più prestatori di servizi di pagamento[12]. Secondo quanto affermato al considerando 28 della PSD2, l'utente di servizi di pagamento può disporre immediatamente di un quadro generale della sua situazione finanziaria in un dato momento.

8. Per quanto riguarda i servizi di informazione sui conti, i servizi offerti potrebbero essere di diversi tipi e porre l'accento su caratteristiche e finalità differenti. Alcuni prestatori possono ad esempio offrire agli utenti servizi di pianificazione del bilancio e di monitoraggio della spesa. Il trattamento dei dati personali nell'ambito di tali servizi è disciplinato dalla PSD2. I servizi che comportano valutazioni del merito creditizio dell'utente di servizi di pagamento o i servizi di audit che si basano sulla raccolta di informazioni tramite un servizio di informazione sui conti esulano dall'ambito di applicazione della PSD2 e rientrano pertanto nell'ambito di applicazione del GDPR. Inoltre anche i conti diversi dai conti di pagamento (ad esempio i conti di risparmio e di investimento) non sono contemplati dalla PSD2. In ogni caso, il GDPR è il quadro giuridico applicabile al trattamento dei dati personali.

Esempio 1
HappyPayments è un'impresa che offre un servizio online che consiste nella fornitura di informazioni su uno o più conti di pagamento tramite un'applicazione mobile per consentire il controllo della propria situazione finanziaria (servizio di informazione sui conti). Attraverso tale servizio, l'utente di servizi di pagamento può visualizzare in forma sintetica il saldo e le operazioni recenti relativamente a due o più conti di pagamento detenuti presso banche differenti. Il servizio consente inoltre, a discrezione dell'utente di servizi di pagamento, di classificare le spese e le entrate in funzione di diverse categorie (stipendio, tempo libero, energia, mutuo, ecc.), aiutando così l'utente di servizi di pagamento nella pianificazione finanziaria. Attraverso l'applicazione in questione, HappyPayments offre anche un servizio che dispone pagamenti direttamente dal conto o dai conti di pagamento designati dall'utente (servizio di disposizione di ordine di pagamento).

9. La PSD2 disciplina le condizioni giuridiche alle quali i PISP e gli AISP possono accedere ai conti di pagamento allo scopo di fornire i rispettivi servizi agli utenti di servizi di pagamento.

10. L'articolo 66, paragrafo 1, e l'articolo 67, paragrafo 1, della PSD2 stabiliscono che l'accesso e l'utilizzo dei servizi di pagamento e di informazione sui conti sono diritti dell'utente di servizi di pagamento. Ciò significa che l'utente di servizi di pagamento dovrebbe rimanere totalmente libero per quanto riguarda l'esercizio di tale diritto e non può essere costretto ad avvalersene.

11. L'accesso ai conti di pagamento e l'uso delle informazioni sui conti di pagamento sono in parte disciplinati dagli articoli 66 e 67 della PSD2, che contengono garanzie relative alla protezione dei dati (personali). L'articolo 66, paragrafo 3, lettera f), della PSD2 stabilisce che il PISP non può chiedere all'utente di servizi di pagamento dati diversi da quelli necessari a prestare il servizio di disposizione di ordine di pagamento, e l'articolo 66, paragrafo 3, lettera g), della PSD2 stabilisce che i PISP non possono usare o conservare dati né accedere ad essi per fini diversi dalla prestazione del servizio di disposizione di ordine di pagamento esplicitamente richiesto dall'utente di servizi di pagamento. L'articolo 67, paragrafo 2, lettera d), della PSD2 limita inoltre l'accesso degli AISP alle

[12] Articolo 4, punto 16), della PSD2.

informazioni sui conti di pagamento designati e sulle operazioni di pagamento a questi associate, mentre l'articolo 67, paragrafo 2, lettera f), della PSD2 stabilisce che gli AISP non possono usare o conservare dati né accedere ad essi per fini diversi da quelli della prestazione del servizio di informazione sui conti esplicitamente richiesto dall'utente di servizi di pagamento, conformemente alle norme sulla protezione dei dati. L'articolo sottolinea che, nell'ambito dei servizi di informazione sui conti, i dati personali possono essere raccolti solo per finalità determinate, esplicite e legittime. Un AISP dovrebbe pertanto indicare esplicitamente nel contratto per quali finalità specifiche saranno trattati i dati personali relativi alle informazioni sui conti nell'ambito del servizio di informazione sui conti prestato. Il contratto dovrebbe essere lecito, corretto e trasparente ai sensi dell'articolo 5 del GDPR e dovrebbe rispettare anche le altre normative in materia di protezione dei consumatori.

12. A seconda delle circostanze specifiche, i prestatori di servizi di pagamento potrebbero essere titolari del trattamento o responsabili del trattamento ai sensi del GDPR. Ai fini delle presenti linee guida, sono "titolari del trattamento" i prestatori di servizi di pagamento che, singolarmente o insieme ad altri, determinano le finalità e i mezzi del trattamento di dati personali. Ulteriori orientamenti al riguardo sono consultabili nelle linee guida 7/2020 dell'EDPB sulle nozioni di titolare del trattamento e responsabile del trattamento nel GDPR.

2 FONDAMENTI DI LICEITA' E ULTERIORE TRATTAMENTO A NORMA DELLA PSD2

2.1 Fondamenti di liceità del trattamento

13. A norma del GDPR, i titolari del trattamento devono disporre di una base giuridica per trattare i dati personali. All'articolo 6, paragrafo 1, del GDPR figura un elenco esaustivo e restrittivo di sei basi giuridiche per il trattamento dei dati personali a norma del regolamento[13]. Spetta al titolare del trattamento definire la base giuridica adatta e garantire che siano soddisfatte tutte le condizioni per l'applicazione di tale base giuridica. La determinazione della base adatta e più appropriata in una specifica situazione dipende dalle circostanze in cui avviene il trattamento, comprese la finalità del trattamento e la relazione intercorrente tra il titolare del trattamento e l'interessato.

2.2 Articolo 6, paragrafo 1, lettera b), del GDPR (il trattamento è necessario all'esecuzione di un contratto)

14. I servizi di pagamento sono prestati sulla base di un contratto tra l'utente di servizi di pagamento e il prestatore di servizi di pagamento. Come affermato al considerando 87 della PSD2, "*[l]a presente direttiva dovrebbe riguardare solo gli obblighi e le responsabilità contrattuali tra l'utente dei servizi di pagamento e il corrispondente prestatore di servizi di pagamento*". Nell'ambito del GDPR, la principale base giuridica per il trattamento dei dati personali per la prestazione di servizi di pagamento è l'articolo 6, paragrafo 1, lettera b), per cui il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso.

15. I servizi di pagamento disciplinati dalla PSD2 sono definiti all'allegato I della stessa. La prestazione di tali servizi, quale definita dalla PSD2, è un requisito per la conclusione di un contratto in cui le parti hanno accesso ai dati relativi al conto di pagamento dell'utente di servizi di pagamento. I prestatori di servizi di pagamento in questione devono inoltre essere operatori autorizzati. Per quanto riguarda i servizi di disposizione di ordine di pagamento e i servizi di informazione sui conti ai sensi della PSD2, i contratti possono includere clausole che stabiliscono anche condizioni relative a servizi aggiuntivi non disciplinati dalla PSD2. Le *linee guida 2/2019 dell'EDPB sul*

[13] A norma dell'articolo 6, il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:
(a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
(b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
(c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
(d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
(e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
(f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del regolamento generale sulla protezione dei dati nel contesto della fornitura di servizi online agli interessati chiariscono che i titolari del trattamento devono valutare quale trattamento di dati personali sia oggettivamente necessario per eseguire il contratto. Tali linee guida sottolineano che la giustificazione della necessità dipende dalla natura del servizio, dalle prospettive e dalle aspettative reciproche delle parti contraenti, dalla ratio del contratto e dai suoi elementi essenziali.

16. Le linee guida 2/2019 dell'EDPB chiariscono inoltre che, alla luce dell'articolo 7, paragrafo 4, del GDPR, viene operata una distinzione tra le attività di trattamento necessarie all'esecuzione di un contratto e le clausole che subordinano l'erogazione del servizio a talune attività di trattamento che di fatto non sono necessarie ai fini dell'esecuzione del contratto. Il concetto di "necessario all'esecuzione" richiede chiaramente qualcosa di più di una clausola contrattuale[14]. Il titolare del trattamento dovrebbe essere in grado di dimostrare in che modo l'oggetto principale del contratto specifico stipulato con l'interessato non sia di fatto realizzabile senza lo specifico trattamento dei dati personali in questione. Un mero riferimento al trattamento dei dati o la semplice menzione di tale trattamento in un contratto non è sufficiente a far rientrare il trattamento in questione nell'ambito di applicazione dell'articolo 6, paragrafo 1, lettera b), del GDPR.

17. L'articolo 5, paragrafo 1, lettera b), del GDPR stabilisce il principio della limitazione delle finalità, che impone che i dati personali siano raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità. Nel valutare se l'articolo 6, paragrafo 1, lettera b), costituisca una base giuridica appropriata per un servizio (di pagamento) online, si dovrebbe tenere conto dello scopo, della finalità o dell'obiettivo specifico/a del servizio[15]. Le finalità del trattamento devono essere chiaramente specificate e comunicate all'interessato, nel rispetto degli obblighi di limitazione delle finalità e di trasparenza cui il titolare del trattamento è soggetto. La valutazione di ciò che è "necessario" comporta una valutazione combinata, basata sui fatti, del trattamento "per l'obiettivo perseguito e della possibilità che tale trattamento sia meno intrusivo rispetto ad altre opzioni disponibili per il conseguimento del medesimo obiettivo". L'articolo 6, paragrafo 1, lettera b), non si applicherà al trattamento che è utile, ma non oggettivamente necessario per eseguire il servizio oggetto del contratto o per adottare le pertinenti misure precontrattuali su richiesta dell'interessato, anche laddove ciò sia necessario per altre finalità commerciali del titolare del trattamento[16].

18. Le linee guida 2/2019 dell'EDPB chiariscono che un contratto non può ampliare artificiosamente le categorie di dati personali o le tipologie di trattamenti che il titolare necessita di effettuare per l'esecuzione del contratto ai sensi dell'articolo 6, paragrafo 1, lettera b)[17]. In tali linee guida vengono trattati anche i casi in cui si possono creare situazioni del tipo "prendere o lasciare" per gli interessati che intendono usufruire soltanto di uno dei servizi. Ciò può verificarsi quando un titolare del trattamento desidera raggruppare più servizi distinti o elementi di un servizio con finalità, caratteristiche o ratio differenti in un unico contratto. Se il contratto è costituito da più servizi o elementi distinti che di fatto possono ragionevolmente essere prestati indipendentemente l'uno dall'altro, l'applicabilità dell'articolo 6, paragrafo 1, lettera b), dovrebbe essere valutata separatamente nel contesto di ciascuno di tali servizi, considerando ciò che è

[14] EDPB, linee guida 2/2019 sul trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del regolamento generale sulla protezione dei dati nel contesto della fornitura di servizi online agli interessati, pag. 8.

[15] Ibidem.

[16] Ibidem, pag. 7.

[17] Ibidem, pag. 10.

oggettivamente necessario per ciascuno dei singoli servizi che l'interessato ha attivamente richiesto o sottoscritto[18].

19. Conformemente alle suddette linee guida, i titolari del trattamento devono valutare ciò che è oggettivamente necessario all'esecuzione del contratto. Se i titolari del trattamento non sono in grado dimostrare che il trattamento dei dati personali relativi al conto di pagamento è oggettivamente necessario per la prestazione di ciascun distinto servizio, l'articolo 6, paragrafo 1, lettera b), del GDPR non costituisce una valida base giuridica per il trattamento. In tali casi, il titolare del trattamento dovrebbe valutare la possibilità di fondare il trattamento su un'altra base giuridica.

2.3 Prevenzione delle frodi

20. A norma dell'articolo 94, paragrafo 1, della PSD2, gli Stati membri devono autorizzare il trattamento dei dati personali da parte di sistemi di pagamento e di prestatori di servizi di pagamento se necessario per garantire la prevenzione, l'indagine e l'individuazione dei casi di frode nei pagamenti. Il trattamento dei dati personali strettamente necessario per prevenire le frodi potrebbe costituire un interesse legittimo del prestatore di servizi di pagamento in questione, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato[19]. Le attività di trattamento ai fini della prevenzione delle frodi dovrebbero basarsi su un'attenta valutazione caso per caso da parte del titolare del trattamento, conformemente al principio di responsabilizzazione. Inoltre i titolari del trattamento possono anche essere soggetti a specifici obblighi giuridici che richiedono il trattamento di dati personali allo scopo di prevenire le frodi.

2.4 Ulteriore trattamento (AISP e PISP)

21. L'articolo 6, paragrafo 4, del GDPR stabilisce le condizioni affinché i dati personali possano essere trattati per una finalità diversa da quella per la quale sono stati raccolti. Più nello specifico, tale ulteriore trattamento può avere luogo se si basa su un atto legislativo dell'Unione o degli Stati membri che costituisce una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1, se l'interessato ha prestato il proprio consenso o se il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti è compatibile con la finalità iniziale.

22. Occorre considerare con attenzione l'articolo 66, paragrafo 3, lettera g), e l'articolo 67, paragrafo 2, lettera f), della PSD2. Come sottolineato in precedenza, l'articolo 66, paragrafo 3, lettera g), della PSD2 stabilisce che il PISP non può usare o conservare dati né accedere ad essi per fini diversi dalla prestazione del servizio di disposizione di ordine di pagamento esplicitamente richiesto dal pagatore. L'articolo 67, paragrafo 2, lettera f), della PSD2 stabilisce che l'AISP non può usare o conservare dati né accedere a essi per fini diversi da quelli della prestazione del servizio di informazione sui conti esplicitamente richiesto dall'utente di servizi di pagamento, conformemente alle norme sulla protezione dei dati.

23. Di conseguenza l'articolo 66, paragrafo 3, lettera g), e l'articolo 67, paragrafo 2, lettera f), della PSD2 limitano considerevolmente le possibilità di trattamento per altre finalità, il che significa che il trattamento per un'altra finalità non è consentito, a meno che l'interessato abbia prestato il proprio consenso a norma dell'articolo 6, paragrafo 1, lettera a), del GDPR o che il trattamento sia previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, a norma dell'articolo 6, paragrafo 4, del GDPR. Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato

[18] Ibidem, pag. 11.
[19] Considerando 47 del GDPR.

o su un atto legislativo dell'Unione o degli Stati membri, le limitazioni di cui all'articolo 66, paragrafo 3, lettera g), e all'articolo 67, paragrafo 2, lettera f), della PSD2 chiariscono che qualsiasi altra finalità non è compatibile con la finalità per la quale i dati personali sono inizialmente raccolti. Il test di compatibilità di cui all'articolo 6, paragrafo 4, del GDPR non può dar luogo a una base giuridica per il trattamento.

24. L'articolo 6, paragrafo 4, del GDPR consente un ulteriore trattamento sulla base del diritto dell'Unione o degli Stati membri. Ad esempio, tutti i PISP e gli AISP sono soggetti obbligati ai sensi dell'articolo 3, punto 2), lettera a), della direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio, del 20 maggio 2015, relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo. Tali soggetti obbligati sono pertanto tenuti ad applicare le misure di adeguata verifica della clientela specificate nella direttiva. I dati personali trattati nell'ambito di un servizio disciplinato dalla PSD2 sono dunque soggetti a un ulteriore trattamento sulla base di almeno un obbligo giuridico gravante sul prestatore di servizi[20].

25. Come indicato al punto 20, l'articolo 6, paragrafo 4, del GDPR prevede che il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti possa basarsi sul consenso dell'interessato, qualora siano soddisfatte tutte le condizioni per la prestazione del consenso stabilite dal regolamento. Come sottolineato in precedenza, il titolare del trattamento deve dimostrare che sussiste la possibilità di rifiutare o revocare il consenso senza subire un pregiudizio (considerando 42 del GDPR).

2.5 Motivo lecito per concedere l'accesso al conto (ASPSP)

26. Come sottolineato al punto 10, gli utenti di servizi di pagamento possono esercitare il diritto di avvalersi di servizi di disposizione di ordine di pagamento e di informazione sui conti. Gli obblighi gravanti sugli Stati membri a norma dell'articolo 66, paragrafo 1, e dell'articolo 67, paragrafo 1, della PSD2 dovrebbero essere recepiti nell'ordinamento nazionale al fine di garantire l'efficace applicazione del diritto dell'utente di servizi di pagamento di beneficiare dei suddetti servizi di pagamento. L'effettiva applicazione di tali diritti non sarebbe possibile senza l'esistenza di un corrispondente obbligo per l'ASPSP, generalmente una banca, di concedere l'accesso al conto al prestatore di servizi di pagamento, a condizione che quest'ultimo soddisfi tutti i requisiti per ottenere l'accesso al conto dell'utente di servizi di pagamento. Inoltre l'articolo 66, paragrafo 5, e l'articolo 67, paragrafo 4, della PSD2 stabiliscono chiaramente che la prestazione di servizi di disposizione di ordine di pagamento e di servizi di informazione sui conti non è subordinata all'esistenza di un rapporto contrattuale tra il PISP/AISP e l'ASPSP.

27. Il trattamento di dati personali da parte dell'ASPSP che consiste nel concedere l'accesso ai dati personali richiesti dal PISP e dall'AISP affinché essi possano prestare i propri servizi di pagamento all'utente di servizi di pagamento si basa su un obbligo giuridico. Per conseguire gli obiettivi della PSD2, gli ASPSP devono fornire i dati personali ai PISP e agli AISP, condizione necessaria affinché questi ultimi possano prestare i propri servizi, garantendo in tal modo l'applicazione dei diritti di cui all'articolo 66, paragrafo 1, e all'articolo 67, paragrafo 1, della PSD2. La base giuridica applicabile nel caso di specie è dunque l'articolo 6, paragrafo 1, lettera c), del GDPR.

28. Poiché il GDPR specifica che il trattamento basato su un obbligo giuridico dovrebbe essere chiaramente stabilito dal diritto dell'Unione o degli Stati membri (cfr. l'articolo 6, paragrafo 3, del GDPR), l'obbligo per gli ASPSP di concedere l'accesso dovrebbe essere sancito dall'ordinamento nazionale che recepisce la PSD2.

[20] Si noti che un esame approfondito della questione riguardante la conformità o meno della direttiva antiriciclaggio alle norme di cui all'articolo 6, paragrafo 4, del GDPR esula dall'oggetto del presente documento.

3 CONSENSO ESPLICITO

3.1 Consenso ai sensi del GDPR

29. A norma del GDPR, il consenso è una delle sei basi giuridiche che determinano la liceità del trattamento dei dati personali. L'articolo 4, punto 11), del GDPR definisce il consenso come "qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento". Queste quattro condizioni – libero, specifico, informato e inequivocabile – sono essenziali affinché il consenso sia valido. Secondo le linee guida 5/2020 dell'EDPB sul consenso ai sensi del regolamento (UE) 2016/679, il consenso può costituire la base legittima appropriata solo se all'interessato vengono offerti il controllo e l'effettiva possibilità di scegliere se accettare i termini proposti o rifiutarli senza subire pregiudizio. Quando richiede il consenso, il titolare del trattamento deve valutare se questo soddisferà tutti i requisiti per essere valido. Se ottenuto nel pieno rispetto del GDPR, il consenso è uno strumento che fornisce all'interessato il controllo sul trattamento dei dati personali che lo riguardano. In caso contrario, il controllo diventa illusorio e il consenso non costituirà una base giuridica valida per il trattamento, rendendo illecita l'attività di trattamento[21].

30. Il GDPR contiene inoltre ulteriori garanzie all'articolo 7, il quale stabilisce che il titolare del trattamento deve essere in grado di dimostrare l'esistenza di un consenso valido al momento del trattamento. La richiesta di consenso deve altresì essere presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. L'interessato deve inoltre essere informato del diritto di revocare il consenso in qualsiasi momento, con la stessa facilità con cui lo ha accordato.

31. A norma dell'articolo 9 del GDPR, il consenso costituisce una delle eccezioni al divieto generale di trattamento di categorie particolari di dati personali. In tal caso il consenso dell'interessato deve tuttavia essere "esplicito"[22].

32. Secondo le linee guida 5/2020 dell'EDPB sul consenso ai sensi del regolamento (UE) 2016/679, il termine "consenso esplicito" ai sensi del GDPR si riferisce al modo in cui il consenso è espresso dall'interessato e significa che l'interessato deve fornire una dichiarazione esplicita di consenso per finalità di trattamento specifiche. Un modo ovvio per assicurarsi che il consenso sia esplicito consisterebbe nel confermare espressamente il consenso in una dichiarazione scritta. Se del caso, il titolare del trattamento potrebbe assicurarsi che la dichiarazione scritta sia firmata dall'interessato, al fine di dissipare tutti i possibili dubbi e la potenziale mancanza di prove in futuro.

33. In nessun caso il consenso può essere dedotto da dichiarazioni o azioni potenzialmente ambigue. Il titolare del trattamento deve inoltre fare attenzione al fatto che il consenso non può essere ottenuto tramite la stessa azione con cui si accetta un contratto o le condizioni generali di servizio.

3.2 Consenso ai sensi della PSD2

34. L'EDPB rileva che il quadro giuridico relativo al consenso esplicito è complesso, poiché la nozione di "consenso esplicito" figura sia nella PSD2 che nel GDPR. Ciò porta a chiedersi se il "consenso

[21] EDPB, linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679, punto 3.

[22] Cfr. anche il parere 15/2011 sulla definizione di consenso (WP 187), pagg. 6-8, e/o il parere 06/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE (WP 217), pagg. 9, 10, 13 e 14.

esplicito" di cui all'articolo 94, paragrafo 2, della PSD2 debba essere interpretato allo stesso modo del consenso esplicito ai sensi del GDPR.

3.2.1 Consenso esplicito ai sensi dell'articolo 94, paragrafo 2, della PSD2

35. La PSD2 contiene una serie di norme specifiche relative al trattamento dei dati personali, in particolare all'articolo 94, paragrafo 1, che stabilisce che il trattamento dei dati personali ai fini della PSD2 deve essere conforme al diritto dell'UE in materia di protezione dei dati. L'articolo 94, paragrafo 2, della PSD2 stabilisce inoltre che i prestatori di servizi di pagamento possono avere accesso, trattare e conservare i dati personali necessari alla prestazione dei rispettivi servizi di pagamento solo dietro consenso esplicito dell'utente di servizi di pagamento. A norma dell'articolo 33, paragrafo 2, della PSD2, il requisito del consenso esplicito dell'utente di servizi di pagamento non si applica agli AISP. Tuttavia l'articolo 67, paragrafo 2, lettera a), della PSD2 prevede ancora il consenso esplicito affinché gli AISP possano prestare il proprio servizio.

36. Come sottolineato in precedenza, l'elenco delle basi giuridiche per il trattamento a norma del GDPR è esaustivo. Come indicato al punto 14, la base giuridica per il trattamento dei dati personali per la prestazione di servizi di pagamento è, in linea di principio, l'articolo 6, paragrafo 1, lettera b), del GDPR, per cui il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso. Ne consegue che l'articolo 94, paragrafo 2, della PSD2 non può essere considerato una base giuridica supplementare per il trattamento dei dati personali. L'EDPB ritiene che, alla luce di quanto precede, tale paragrafo debba essere interpretato, da un lato, in maniera coerente con il quadro giuridico applicabile in materia di protezione dei dati e, dall'altro, in modo da preservarne l'effetto utile. Il consenso esplicito ai sensi dell'articolo 94, paragrafo 2, della PSD2 dovrebbe pertanto essere considerato un requisito aggiuntivo di natura contrattuale[23] in relazione all'accesso ai dati personali, al loro successivo trattamento e alla loro successiva conservazione ai fini della prestazione di servizi di pagamento e non equivale pertanto al consenso (esplicito) ai sensi del GDPR.

37. Il "consenso esplicito" di cui all'articolo 94, paragrafo 2, della PSD2 è un consenso contrattuale. Ciò implica che l'articolo 94, paragrafo 2, della PSD2 dovrebbe essere interpretato nel senso che, al momento di stipulare un contratto con un prestatore di servizi di pagamento ai sensi della PSD2, gli interessati devono essere pienamente informati delle categorie specifiche di dati personali che saranno trattati. Inoltre devono essere informati della finalità specifica (servizio di pagamento) per la quale i loro dati personali saranno trattati e devono accettare esplicitamente tali clausole. Queste ultime dovrebbero essere chiaramente distinguibili dalle altre materie che sono oggetto del contratto e dovrebbero essere accettate in maniera esplicita dall'interessato.

38. Fondamentale per la nozione di "consenso esplicito" di cui all'articolo 94, paragrafo 2, della PSD2 è l'ottenimento dell'accesso ai dati personali per il loro successivo trattamento e la loro successiva conservazione ai fini della prestazione di servizi di pagamento. Ciò implica che il prestatore di servizi di pagamento[24] non sta ancora trattando i dati personali, ma deve avere accesso a dati personali trattati sotto la responsabilità di un altro titolare del trattamento. Se un utente di servizi di pagamento stipula ad esempio un contratto con un prestatore di servizi di disposizione di ordine di pagamento, tale prestatore deve ottenere l'accesso ai dati personali dell'utente di servizi di pagamento trattati sotto la responsabilità del prestatore di servizi di pagamento di radicamento del conto. L'oggetto del consenso esplicito di cui all'articolo 94, paragrafo 2, della PSD2 è il permesso di accedere a tali dati personali e di trattarli e conservarli in quanto necessari ai fini della

[23] Lettera dell'EDPB relativa alla direttiva PSD2, 5 luglio 2018, pag. 4.
[24] Ciò vale per i servizi da 1 a 7 dell'allegato I della PSD2.

prestazione del servizio di pagamento. Se l'interessato fornisce il consenso esplicito, il prestatore di servizi di pagamento di radicamento del conto è tenuto a concedere l'accesso ai dati personali indicati.

39. Sebbene il consenso di cui all'articolo 94, paragrafo 2, della PSD2 non costituisca una base giuridica per il trattamento dei dati personali, tale consenso è specificamente correlato ai dati personali e alla protezione dei dati e garantisce trasparenza e un certo grado di controllo all'utente di servizi di pagamento[25]. Benché la PSD2 non specifichi le condizioni sostanziali per il consenso ai sensi dell'articolo 94, paragrafo 2, della PSD2, essa dovrebbe essere interpretata, come indicato in precedenza, in maniera coerente con il quadro giuridico applicabile in materia di protezione dei dati e in modo da preservarne l'effetto utile.

40. Per quanto riguarda le informazioni che devono essere fornite dai titolari del trattamento e il requisito di trasparenza, le linee guida del gruppo di lavoro Articolo 29 sulla trasparenza specificano che "*[u]na considerazione centrale al principio della trasparenza evidenziata in queste disposizioni è che l'interessato dovrebbe essere in grado di determinare in anticipo quali siano la portata del trattamento e le relative conseguenze e non dovrebbe successivamente essere colto di sorpresa dalle modalità di utilizzo dei dati personali che lo riguardano*"[26].

41. Inoltre, come richiesto dal principio della limitazione delle finalità, i dati personali devono essere raccolti per finalità determinate, esplicite e legittime (articolo 5, paragrafo 1, lettera b), del GDPR). Se i dati personali sono raccolti per più di una finalità, i titolari del trattamento dovrebbero evitare di indicare un'unica finalità generica per giustificare varie ulteriori attività di trattamento che in realtà sono solo lontanamente collegate all'effettiva finalità iniziale[27]. L'EDPB ha evidenziato, da ultimo in riferimento ai contratti riguardanti servizi online, il rischio di inclusione di condizioni generali di trattamento nei contratti e ha affermato che la finalità della raccolta dai dati dovrebbe essere indicata in maniera chiara e specifica: tale finalità dovrebbe essere sufficientemente dettagliata da consentire di stabilire quale tipo di trattamento è incluso nella finalità specifica e quale no, nonché da consentire di valutare il rispetto della legge e l'applicazione delle garanzie in materia di protezione dei dati[28].

42. Se esaminato alla luce del requisito aggiuntivo del consenso esplicito ai sensi dell'articolo 94, paragrafo 2, della PSD2, ciò implica che i titolari del trattamento devono fornire agli interessati informazioni specifiche ed esplicite sulle finalità specifiche indicate dal titolare del trattamento per la richiesta di accesso, trattamento e conservazione dei loro dati. In linea con l'articolo 94, paragrafo 2, della PSD2, gli interessati devono accettare esplicitamente tali finalità specifiche.

43. Inoltre, come indicato al punto 10, l'EDPB sottolinea che l'utente di servizi di pagamento deve poter scegliere se utilizzare o meno il servizio e non può essere costretto ad avvalersene. Pertanto anche il consenso ai sensi dell'articolo 94, paragrafo 2, della PSD2 deve essere prestato liberamente.

3.3 Conclusioni

[25] L'articolo 94, paragrafo 2, della PSD2 rientra nel capo 4 "Protezione dei dati".

[26] Gruppo di lavoro Articolo 29, linee guida sulla trasparenza ai sensi del regolamento 2016/679, punto 10 (adottate l'11 aprile 2018) – approvate dall'EDPB.

[27] Gruppo di lavoro Articolo 29, parere 03/2013 sulla limitazione delle finalità (WP 203), pag. 16.

[28] Linee guida 2/2019 sul trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del regolamento generale sulla protezione dei dati nel contesto della fornitura di servizi online agli interessati, punto 16 (versione per la consultazione pubblica), e parere 03/2013 del gruppo di lavoro Articolo 29 sulla limitazione delle finalità (WP 203), pagg. 15-16.

44. Il consenso esplicito ai sensi della PSD2 è diverso dal consenso (esplicito) ai sensi del GDPR. Il consenso esplicito ai sensi dell'articolo 94, paragrafo 2, della PSD2 è un requisito aggiuntivo di natura contrattuale. Quando un prestatore di servizi di pagamento necessita di accedere ai dati personali per la prestazione di un servizio di pagamento, è necessario il consenso esplicito dell'utente di servizi di pagamento ai sensi dell'articolo 94, paragrafo 2, della PSD2.

4 TRATTAMENTO DEI DATI DEI TACITI INTERESSATI

4.1 Dati dei taciti interessati

45. Una questione riguardante la protezione dei dati che richiede un esame attento è il trattamento dei cosiddetti "dati dei taciti interessati" (*silent party data*). Nell'ambito del presente documento, i dati dei taciti interessati sono dati personali di interessati che non sono utenti di uno specifico prestatore di servizi di pagamento, ma i cui dati personali sono trattati da tale specifico prestatore di servizi di pagamento ai fini dell'esecuzione di un contratto tra il prestatore e un utente di servizi di pagamento. Ciò si verifica ad esempio nel caso in cui un utente di servizi di pagamento, l'interessato A, si avvale dei servizi di un AISP, e l'interessato B ha effettuato una serie di operazioni di pagamento sul conto di pagamento dell'interessato A. In questo caso, l'interessato B è considerato "tacito interessato" e i suoi dati personali (come il suo numero di conto e l'importo oggetto di tali operazioni) sono considerati "dati del tacito interessato".

4.2 Interesse legittimo del titolare del trattamento

46. L'articolo 5, paragrafo 1, lettera b), del GDPR stabilisce che i dati personali devono essere raccolti solamente per finalità determinate, esplicite e legittime e non possono essere successivamente trattati in modo che sia incompatibile con tali finalità. Inoltre il GDPR prevede che qualsiasi trattamento di dati personali debba essere necessario, proporzionato e in linea con i principi di protezione dei dati, quali la limitazione delle finalità e la minimizzazione dei dati.

47. Il GDPR può consentire il trattamento dei dati dei taciti interessati qualora sia necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi (articolo 6, paragrafo 1, lettera f), del GDPR). Tale trattamento può tuttavia avere luogo solo a condizione che "gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali" non prevalgano rispetto al legittimo interesse del titolare del trattamento.

48. Una base lecita per il trattamento dei dati dei taciti interessati da parte dei PISP e degli AISP – nell'ambito della prestazione di servizi di pagamento di cui alla PSD2 – potrebbe quindi essere il legittimo interesse del titolare del trattamento o di terzi a dare esecuzione al contratto stipulato con l'utente di servizi di pagamento. La necessità di trattare i dati personali dei taciti interessati è limitata e determinata dalle ragionevoli aspettative di tali interessati. Nell'ambito della prestazione dei servizi di pagamento disciplinati dalla PSD2 devono essere adottate misure efficaci e adeguate a garantire che non vengano lesi gli interessi o i diritti e le libertà fondamentali dei taciti interessati e che siano rispettate le ragionevoli aspettative di tali interessati riguardo al trattamento dei loro dati personali. A tale riguardo, il titolare del trattamento (AISP o PISP) deve predisporre le garanzie riguardanti il trattamento necessarie a tutelare i diritti degli interessati. Ciò comprende misure tecniche volte ad assicurare che i dati dei taciti interessati non siano trattati per una finalità diversa da quella per la quale i dati personali sono stati inizialmente raccolti dai PISP e dagli AISP. Se possibile, dovrebbero essere utilizzate anche tecniche di cifratura o altre modalità che consentano di raggiungere un livello adeguato di sicurezza e di minimizzazione dei dati.

4.3 Ulteriore trattamento dei dati personali dei taciti interessati

49. Come sottolineato al punto 29, i dati personali trattati in relazione a un servizio di pagamento disciplinato dalla PSD2 potrebbero essere ulteriormente trattati in funzione di obblighi giuridici gravanti sul prestatore di servizi. Tali obblighi giuridici potrebbero riguardare i dati personali dei taciti interessati.

50. Per quanto riguarda l'ulteriore trattamento dei dati dei taciti interessati sulla base di un legittimo interesse, l'EDPB è del parere che tali dati non possano essere utilizzati per una finalità diversa da quella per la quale i dati personali sono stati raccolti, a meno che ciò non sia previsto dal diritto dell'UE o degli Stati membri. Ottenere il consenso dei taciti interessati non è giuridicamente possibile, poiché per farlo sarebbe necessario raccogliere o trattare i dati personali dei taciti interessati, operazioni per le quali non è possibile ravvisare alcuna base giuridica a norma dell'articolo 6 del GDPR. Nemmeno il criterio di compatibilità di cui all'articolo 6, paragrafo 4, del GDPR può fornire una base per il trattamento dei dati per altre finalità (ad esempio attività di marketing diretto). I diritti e le libertà dei taciti interessati non vengono rispettati se il nuovo titolare del trattamento utilizza i dati personali per altre finalità, tenendo conto del contesto in cui tali dati sono stati raccolti, in particolare dell'assenza di qualsiasi relazione con i taciti interessati[29], dell'assenza di qualsiasi legame tra ogni altra finalità e la finalità per la quale i dati personali sono stati inizialmente raccolti (ossia il fatto che i prestatori di servizi di pagamento necessitano dei dati dei taciti interessati soltanto per dare esecuzione a un contratto con l'altra parte contraente), della natura dei dati personali in questione[30] e del fatto che gli interessati non possono ragionevolmente aspettarsi un ulteriore trattamento né tantomeno sapere quale titolare del trattamento possa trattare i loro dati personali, e date le restrizioni giuridiche al trattamento di cui all'articolo 66, paragrafo 3, lettera g), e all'articolo 67, paragrafo 2, lettera f), della PSD2.

[29] Il considerando 87 della PSD2 afferma che la direttiva riguarda "solo gli obblighi e le responsabilità contrattuali tra l'utente dei servizi di pagamento e il corrispondente prestatore di servizi di pagamento". I dati dei taciti interessati non rientrano pertanto nell'ambito di applicazione della PSD2.

[30] Occorre prestare particolare attenzione al trattamento dei dati personali finanziari, in quanto il trattamento può comportare un aumento del possibile rischio per i diritti e le libertà delle persone fisiche, secondo le linee guida in materia di valutazione d'impatto sulla protezione dei dati.

5 TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI PERSONALI A NORMA DELLA PSD2

5.1 Categorie particolari di dati personali

51. A norma dell'articolo 9, paragrafo 1, del GDPR, "[è] vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona".

52. È opportuno sottolineare che in alcuni Stati membri i pagamenti elettronici sono già ampiamente diffusi e molte persone li preferiscono al contante nelle operazioni quotidiane. Al tempo stesso, le operazioni finanziarie possono rivelare informazioni sensibili su un singolo interessato, comprese quelle relative a categorie particolari di dati personali. Ad esempio, a seconda dei dettagli dell'operazione, eventuali donazioni a partiti o organizzazioni politiche, chiese o parrocchie possono rivelare opinioni politiche e convinzioni religiose. L'affiliazione a un sindacato può essere rivelata dall'addebito di una quota associativa annuale sul conto bancario di una persona. Analizzando le parcelle mediche pagate da un interessato a un professionista del settore medico (ad esempio uno psichiatra) è possibile raccogliere dati personali relativi alla salute. Infine le informazioni su taluni acquisti possono rivelare informazioni relative alla vita sessuale o all'orientamento sessuale di una persona. Come dimostrato da questi esempi, anche singole operazioni possono contenere categorie particolari di dati personali. Inoltre i servizi di informazione sui conti potrebbero avvalersi della profilazione quale definita all'articolo 4, punto 4), del GDPR. Come già sottolineato dalle linee guida del gruppo di lavoro Articolo 29 sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679, approvate dall'EDPB, "la profilazione può creare dati appartenenti a categorie particolari desumendoli da dati che di per sé non appartengono a categorie particolari ma che diventano tali se combinati con altri dati."[31] Ciò significa che da un insieme di operazioni finanziarie possono emergere diversi tipi di modelli comportamentali, che possono includere categorie particolari di dati personali. È pertanto molto probabile che un prestatore di servizi che tratta informazioni relative alle operazioni finanziarie degli interessati tratti anche categorie particolari di dati personali.

53. Per quanto riguarda il termine "dati sensibili relativi ai pagamenti", l'EDPB osserva quanto segue. La definizione dei dati sensibili relativi ai pagamenti contenuta nella PSD2 diverge notevolmente dall'accezione del termine "dati personali sensibili" come comunemente utilizzata nell'ambito del GDPR e della (normativa sulla) protezione dei dati. Mentre la PSD2 definisce i dati sensibili relativi ai pagamenti come "dati che possono essere usati per commettere frodi, incluse le credenziali di sicurezza personalizzate", il GDPR sottolinea la necessità di prevedere una specifica protezione per categorie particolari di dati personali che, a norma dell'articolo 9, sono per loro natura particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, come le categorie particolari di dati personali[32]. A tale riguardo si raccomanda almeno di mappare e classificare con precisione il tipo di dati personali che saranno trattati. Molto probabilmente sarà necessaria una valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 del GDPR, che contribuirà

[31] Gruppo di lavoro Articolo 29 per la protezione dei dati, linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679, WP 251 rev.01, pag. 15.

[32] Ad esempio, al considerando 10 del GDPR si fa riferimento a categorie particolari di dati personali con il termine "dati sensibili".

a tale esercizio di mappatura. Ulteriori orientamenti sulle valutazioni d'impatto sulla protezione dei dati sono consultabili nelle linee guida del gruppo di lavoro Articolo 29 in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679, approvate dall'EDPB.

5.2 Deroghe possibili

54. Il divieto di cui all'articolo 9 del GDPR non è assoluto. In particolare, mentre le deroghe di cui all'articolo 9, paragrafo 2, lettere da b) a f) e da h) a j), del GDPR non sono evidentemente applicabili al trattamento dei dati personali nell'ambito della PSD2, si potrebbero prendere in considerazione le due seguenti deroghe di cui all'articolo 9, paragrafo 2, del GDPR:

a) il divieto non si applica se l'interessato ha prestato il proprio consenso esplicito al trattamento dei dati personali in questione per una o più finalità specifiche (articolo 9, paragrafo 2, lettera a), del GDPR);

b) il divieto non si applica se il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato (articolo 9, paragrafo 2, lettera g), del GDPR).

55. È opportuno sottolineare che l'elenco delle deroghe di cui all'articolo 9, paragrafo 2, del GDPR è esaustivo. La possibilità che categorie particolari di dati personali siano incluse nei dati personali trattati per la prestazione di uno qualsiasi dei servizi che rientrano nell'ambito di applicazione della PSD2 deve essere riconosciuta dal prestatore di servizi. Poiché il divieto di cui all'articolo 9, paragrafo 1, del GDPR è applicabile a tali prestatori di servizi, questi ultimi devono garantire che una delle deroghe di cui all'articolo 9, paragrafo 2, del GDPR sia applicabile alla loro situazione. È opportuno sottolineare che, qualora il prestatore di servizi non sia in grado di dimostrare l'applicazione di una delle deroghe, vige il divieto di cui all'articolo 9, paragrafo 1.

5.3 Interesse pubblico rilevante

56. I servizi di pagamento possono trattare categorie particolari di dati personali per motivi di interesse pubblico rilevante, ma solo quando sono soddisfatte tutte le condizioni di cui all'articolo 9, paragrafo 2, lettera g), del GDPR. Ciò significa che il trattamento delle categorie particolari di dati personali deve essere l'oggetto di una specifica deroga all'articolo 9, paragrafo 1, del GDPR sancita dal diritto dell'Unione o degli Stati membri. Tale disposizione dovrà essere proporzionata alla finalità perseguita dal trattamento e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato. La disposizione sancita dal diritto dell'Unione o degli Stati membri dovrà inoltre rispettare l'essenza del diritto alla protezione dei dati. Infine occorre dimostrare anche che il trattamento delle categorie particolari di dati è necessario per motivi di interesse pubblico rilevante, compresi interessi di importanza sistemica. Solo laddove tutte le suddette condizioni siano pienamente soddisfatte, la deroga potrebbe essere applicata a determinati tipi di servizi di pagamento.

5.4 Consenso esplicito

57. Nei casi in cui non trova applicazione la deroga di cui all'articolo 9, paragrafo 2, lettera g), del GDPR, ottenere il consenso esplicito dell'interessato nel rispetto delle condizioni stabilite nel GDPR affinché il consenso sia valido sembra rimanere l'unica possibile deroga lecita per il trattamento delle categorie particolari di dati personali da parte di prestatori terzi. Le linee guida 5/2020

dell'EDPD sul consenso ai sensi del regolamento (UE) 2016/679 affermano[33] che "[l]'articolo 9, paragrafo 2, non riconosce il trattamento "necessario all'esecuzione di un contratto" come un'eccezione al divieto generale di trattare categorie particolari di dati. Di conseguenza i titolari del trattamento e gli Stati membri che rientrano nel contesto di applicazione di tale circostanza dovrebbero esaminare le eccezioni specifiche di cui all'articolo 9, paragrafo 2, lettere da b) a j)". Quando i prestatori di servizi si basano sull'articolo 9, paragrafo 2, lettera a), del GDPR, devono assicurarsi che sia stato loro accordato il consenso esplicito prima di iniziare il trattamento. Il consenso esplicito di cui all'articolo 9, paragrafo 2, lettera a), del GDPR deve soddisfare tutti i requisiti stabiliti dal regolamento.

5.5 Assenza di deroghe applicabili

58. Come sottolineato in precedenza, qualora il prestatore di servizi non sia in grado di dimostrare l'applicabilità di una delle deroghe, vige il divieto di cui all'articolo 9, paragrafo 1. In questo caso si potrebbero adottare misure tecniche volte a impedire il trattamento di categorie particolari di dati personali, ad esempio impedendo il trattamento di alcuni punti dati. A tale riguardo, i prestatori di servizi di pagamento possono esaminare le opzioni tecniche disponibili per escludere categorie particolari di dati personali e consentire un accesso selezionato che impedisca il trattamento di categorie particolari di dati personali relativi a taciti interessati da parte di prestatori terzi.

[33] EDPB, linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679, punto 99.

6 MINIMIZZAZIONE DEI DATI, SICUREZZA, TRASPARENZA, RESPONSABILIZZAZIONE E PROFILAZIONE

6.1 Minimizzazione dei dati e protezione dei dati fin dalla progettazione e per impostazione predefinita

59. Il principio della minimizzazione dei dati è sancito dall'articolo 5, paragrafo 1, lettera c), del GDPR: "I dati personali sono [...] adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati". In base al principio della minimizzazione dei dati, i titolari del trattamento essenzialmente non dovrebbero trattare più dati personali di quanto necessario per conseguire la specifica finalità perseguita. Come indicato nel capitolo 2, la quantità e il tipo di dati personali necessari per prestare il servizio di pagamento sono determinati dall'obiettivo e dall'oggetto essenziale del contratto come inteso da entrambe le parti[34]. La minimizzazione dei dati è applicabile a ogni trattamento (ad esempio a ogni raccolta o richiesta di dati personali o a ogni accesso a dati personali). Le linee guida 4/2019 dell'EDPB sulla protezione dei dati fin dalla progettazione e per impostazione predefinita a norma dell'articolo 25 del GDPR stabiliscono che anche i responsabili del trattamento e i fornitori di tecnologie sono riconosciuti come promotori essenziali della protezione dei dati fin dalla progettazione e per impostazione predefinita; essi dovrebbero inoltre essere consapevoli del fatto che i titolari del trattamento sono tenuti a trattare i dati personali solo con sistemi e tecnologie caratterizzati da una protezione dei dati integrata[35].

60. L'articolo 25 del GDPR sancisce l'obbligo di applicazione della protezione dei dati fin dalla progettazione e per impostazione predefinita. Tale obbligo è particolarmente importante per il principio della minimizzazione dei dati. A norma del suddetto articolo, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate, volte ad attuare in modo efficace i principi di protezione dei dati e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del GDPR e tutelare i diritti degli interessati. Il titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. Tali misure possono comprendere la cifratura, la pseudonimizzazione e altre misure tecniche.

61. Quando si applica l'obbligo di cui all'articolo 25 del GDPR, occorre tenere conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche dei rischi di probabilità e gravità variabili per i diritti e le libertà delle persone fisiche comportati dal trattamento. Ulteriori chiarimenti in merito a tale obbligo vengono forniti nelle già menzionate linee guida 4/2019 dell'EDPB sulla protezione dei dati fin dalla progettazione e per impostazione predefinita a norma dell'articolo 25.

6.2 Misure di minimizzazione dei dati

62. Il prestatore terzo che accede ai dati del conto di pagamento al fine di fornire i servizi richiesti deve tenere conto anche del principio di minimizzazione dei dati e deve raccogliere solo i dati personali necessari per fornire gli specifici servizi di pagamento richiesti dall'utente di servizi di pagamento.

---

[34] EDPB, linee guida 2/2019 sul trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del regolamento generale sulla protezione dei dati nel contesto della fornitura di servizi online agli interessati, punto 32.

[35] *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, pag. 29.

In linea di principio, l'accesso ai dati personali dovrebbe essere limitato a quanto necessario per la prestazione dei servizi di pagamento. Come sottolineato nel capitolo 2, a norma della PSD2 gli ASPSP sono tenuti a condividere le informazioni dell'utente di servizi di pagamento su richiesta di quest'ultimo, quando questi intenda utilizzare un servizio di disposizione di ordine di pagamento o un servizio di informazione sui conti.

63. Qualora non tutti i dati relativi al conto di pagamento siano necessari per l'esecuzione del contratto, l'AISP dovrebbe selezionare le categorie di dati pertinenti prima che i dati vengano raccolti. Tra le categorie di dati che potrebbero non essere necessarie possono figurare ad esempio l'identità del tacito interessato e le caratteristiche dell'operazione. Inoltre, a meno che non sia richiesto dal diritto degli Stati membri o dell'Unione, può non essere necessario indicare l'IBAN del conto bancario del tacito interessato.

64. A tale proposito potrebbe essere presa in considerazione, nell'ambito dell'attuazione di politiche adeguate in materia di protezione dei dati, in linea con l'articolo 24, paragrafo 2, del GDPR, l'eventuale applicazione di misure tecniche che consentano o favoriscano l'adempimento dell'obbligo, da parte dei prestatori terzi, di accedere e reperire solo i dati personali necessari per la fornitura dei loro servizi. A tale riguardo, l'EDPB raccomanda l'uso di strumenti digitali che aiutino gli AISP a ottemperare all'obbligo di raccogliere solo i dati personali necessari per le finalità per le quali viene effettuato il trattamento. Ad esempio, quando un prestatore di servizi non necessita delle caratteristiche delle operazioni (indicate nel campo delle registrazioni destinato alla descrizione delle operazioni) per la fornitura del suo servizio, uno strumento digitale di selezione potrebbe consentire ai prestatori terzi di escludere il campo in questione dalle attività di trattamento complessive da loro svolte.

Esempio 2

HappyPayments, il prestatore di servizi di informazione sui conti di cui all'esempio 1, vuole assicurarsi di trattare solo i dati personali relativi ai conti di pagamento cui i suoi utenti sono interessati. Chiedere l'accesso a un maggior numero di dati relativi ai conti di pagamento non sarebbe infatti necessario per la prestazione del servizio. HappyPayments consente dunque agli utenti di selezionare le tipologie specifiche di informazioni cui sono interessati.

L'utente A vuole avere una visione d'insieme delle proprie spese negli ultimi due mesi. Pertanto richiede, in relazione ai suoi due conti bancari, detenuti presso due diversi ASPSP, le informazioni riguardanti tutte le operazioni degli ultimi due mesi, l'importo delle operazioni, la data di esecuzione e il nome del destinatario, e seleziona le caselle corrispondenti nell'interfaccia utente di HappyPayments.

HappyPayments inizia dunque a richiedere ai rispettivi ASPSP solo le informazioni corrispondenti ai campi selezionati dall'utente A e solo per il periodo degli ultimi due mesi. Non vengono richieste informazioni quali la "comunicazione" del trasferimento o l'IBAN, in quanto l'utente A non ha richiesto tali informazioni.

Per permettere a HappyPayments di ottemperare ai propri obblighi di minimizzazione dei dati, gli ASPSP consentono a HappyPayments di richiedere campi specifici per una serie di date.

65. A tale proposito è inoltre opportuno osservare che, a norma della PSD2, gli ASPSP sono autorizzati a fornire l'accesso solo alle informazioni sui conti di pagamento. La PSD2 non prevede alcuna base giuridica che consenta l'accesso ai dati personali contenuti in altri conti, quali conti di risparmio, conti ipotecari o conti di investimento. Di conseguenza, a norma della PSD2, devono essere attuate misure tecniche per garantire che l'accesso sia limitato alle informazioni sui conti di pagamento necessarie.

66. Oltre a raccogliere il minor numero possibile di dati, il prestatore di servizi deve anche applicare periodi di conservazione limitati. I dati personali non dovrebbero essere conservati dal prestatore di servizi per un periodo superiore a quello necessario per le finalità indicate dall'utente di servizi di pagamento.

67. Se il contratto tra l'interessato e l'AISP richiede la trasmissione di dati personali a terzi, possono essere trasmessi solo i dati personali necessari per l'esecuzione del contratto. Gli interessati dovrebbero inoltre essere specificamente informati della trasmissione e dei dati personali che saranno trasmessi ai terzi in questione.

6.3 Sicurezza

68. L'EDPB ha già sottolineato che la violazione dei dati personali finanziari "*implica chiaramente gravi ripercussioni sulla vita quotidiana dell'interessato*" e cita a titolo di esempio i rischi di frodi relative ai pagamenti[36].

69. Se una violazione dei dati riguarda dati finanziari, l'interessato può essere esposto a rischi considerevoli. A seconda delle informazioni violate, gli interessati possono essere esposti al rischio di furto d'identità e furto dei fondi nei loro conti e di altri beni. Vi è inoltre la possibilità che l'esposizione dei dati sulle operazioni comporti notevoli rischi per la privacy, in quanto i dati relativi alle operazioni possono contenere riferimenti a tutti gli aspetti della vita privata dell'interessato. Allo stesso tempo, i dati finanziari sono ovviamente preziosi per i criminali e rappresentano quindi un bersaglio allettante.

70. In qualità di titolari del trattamento, i prestatori di servizi di pagamento sono tenuti ad adottare misure adeguate per proteggere i dati personali degli interessati (articolo 24, paragrafo 1, del GDPR). Quanto più alti sono i rischi associati all'attività di trattamento svolta dal titolare del trattamento, tanto più rigorose sono le norme di sicurezza che devono essere applicate. Poiché il trattamento dei dati finanziari è collegato a una serie di gravi rischi, le misure di sicurezza dovrebbero essere conseguentemente rigorose.

71. I fornitori di servizi dovrebbero essere tenuti a rispettare norme severe, compresi meccanismi di autenticazione forte del cliente e norme di sicurezza rigorose per i dispositivi tecnici[37]. Sono importanti anche altre procedure, come la verifica delle norme di sicurezza e delle procedure operative contro l'accesso non autorizzato predisposte dai responsabili del trattamento.

6.4 Trasparenza e responsabilizzazione

72. La trasparenza e la responsabilizzazione sono due principi fondamentali del GDPR.

73. Per quanto riguarda la trasparenza (articolo 5, paragrafo 1, lettera a), del GDPR), l'articolo 12 del GDPR specifica che i titolari del trattamento devono adottare misure appropriate per fornire tutte le informazioni di cui agli articoli 13 e 14 del regolamento. Inoltre, a norma dello stesso articolo, le informazioni o le comunicazioni riguardanti il trattamento dei dati personali devono essere concise, trasparenti, intelligibili e facilmente accessibili. Le informazioni devono essere formulate con un linguaggio semplice e chiaro e devono essere fornite per iscritto "o con altri mezzi, anche, se del caso, con mezzi elettronici". Le linee guida del gruppo di lavoro Articolo 29 sulla trasparenza ai sensi del regolamento 2016/679, approvate dal comitato europeo per la protezione dei dati,

[36] Gruppo di lavoro Articolo 29, linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679, WP 248 rev.01, approvate dall'EDPB.

[37] Si vedano le norme tecniche di regolamentazione.

forniscono orientamenti specifici riguardanti il rispetto del principio di trasparenza negli ambienti digitali.

74. Secondo le suddette linee guida sulla trasparenza ai sensi del regolamento 2016/679, l'articolo 11 del GDPR dovrebbe essere interpretato come un modo per realizzare un'effettiva minimizzazione dei dati senza ostacolare l'esercizio dei diritti dell'interessato e tale esercizio dovrebbe essere reso possibile con l'ausilio delle ulteriori informazioni fornite dall'interessato. Vi possono essere situazioni in cui il titolare tratta dati personali che non richiedono l'identificazione dell'interessato (ad esempio dati pseudonimizzati). In tali casi, può risultare pertinente anche l'articolo 11, paragrafo 1, dal momento che afferma che il titolare del trattamento non è obbligato a conservare, acquisire o trattare ulteriori informazioni per identificare l'interessato al solo fine di rispettare il GDPR.

75. Per i servizi di cui alla PSD2, l'articolo 13 del GDPR si applica ai dati personali raccolti presso l'interessato, mentre l'articolo 14 si applica qualora i dati personali non siano stati ottenuti presso l'interessato.

76. L'interessato deve essere informato in particolare del periodo di conservazione dei dati personali oppure, se ciò non è possibile, dei criteri utilizzati per determinare tale periodo e, se del caso, dei legittimi interessi perseguiti dal titolare del trattamento o da eventuali terzi. Qualora il trattamento sia basato sul consenso di cui all'articolo 6, paragrafo 1, lettera a), del GDPR o sul consenso esplicito di cui all'articolo 9, paragrafo 2, lettera a), del GDPR, l'interessato deve essere informato dell'esistenza del diritto di revocare il consenso in qualsiasi momento.

77. Il titolare del trattamento deve fornire le informazioni all'interessato, tenendo conto delle specifiche circostanze in cui i dati personali sono trattati. Nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato[38], circostanza che riguarderà probabilmente gli AISP, le informazioni devono essere fornite al più tardi al momento della prima comunicazione all'interessato. Se i dati personali devono essere comunicati a un altro destinatario, le informazioni devono essere fornite al più tardi al momento della prima comunicazione dei dati personali.

78. Per quanto riguarda i servizi di pagamento online, le suddette linee guida chiariscono che i titolari del trattamento possono adottare un approccio stratificato, optando per una combinazione di metodi al fine di assicurare la trasparenza. Si raccomanda in particolare l'impiego di dichiarazioni/informative sulla privacy stratificate per collegare le varie categorie di informazioni da fornire all'interessato, piuttosto che l'inserimento di tutte le informazioni in un'unica informativa su una schermata, così da evitare un sovraccarico di informazioni e garantire nel contempo l'efficacia delle stesse.

79. Le suddette linee guida chiariscono inoltre che i titolari del trattamento possono scegliere di utilizzare strumenti aggiuntivi per fornire informazioni al singolo interessato, come ad esempio i dashboard ("cruscotti di controllo") per la privacy. Un dashboard per la privacy è un punto unico dal quale l'interessato può visualizzare le "informazioni sulla privacy" e gestire le proprie preferenze permettendo o impedendo al titolare del trattamento in questione determinati usi dei dati che lo riguardano[39]. Un dashboard per la privacy potrebbe fornire una panoramica dei

[38] Articolo 14, paragrafo 3, lettera b), del GDPR.

[39] Secondo le linee guida del gruppo di lavoro Articolo 29 sulla trasparenza ai sensi del regolamento 2016/679, approvate dall'EDPB, i dashboard per la privacy sono particolarmente utili quando gli interessati usano lo stesso servizio su diversi dispositivi, poiché consentono loro di accedere ai loro dati personali e di controllarli,

prestatori terzi che hanno ottenuto il consenso esplicito dell'interessato, nonché informazioni pertinenti sulla natura e sulla quantità di dati personali cui i prestatori terzi hanno avuto accesso. In linea di principio, l'ASPSP può offrire all'utente la possibilità di revocare uno specifico consenso esplicito a norma della PSD2[40] attraverso la panoramica, negando così a uno o più prestatori terzi l'accesso ai propri conti di pagamento. L'utente potrebbe inoltre chiedere a un ASPSP di negare l'accesso ai propri conti di pagamento a uno o più prestatori terzi specifici[41], in quanto l'utente ha il diritto di (non) avvalersi di un servizio di informazione sui conti. Se i dashboard per la privacy vengono utilizzati per accordare o revocare un consenso esplicito, dovrebbero essere progettati e applicati a norma di legge, evitando in particolare di limitare il diritto dei prestatori terzi di fornire servizi conformemente alla PSD2. A tale riguardo e in conformità delle disposizioni applicabili a norma della PSD2, un prestatore terzo ha la possibilità di ottenere nuovamente il consenso esplicito dell'utente dopo che tale consenso è stato revocato.

80. I principi di responsabilizzazione impongono al titolare del trattamento di mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR, in particolare ai principi fondamentali di protezione dei dati di cui all'articolo 5, paragrafo 1. Tali misure dovrebbero tenere conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento nonché dei rischi per i diritti e le libertà delle persone fisiche e devono essere riesaminate e aggiornate qualora necessario[42].

6.5 Profilazione

81. Il trattamento dei dati personali da parte dei prestatori di servizi di pagamento può comportare una "profilazione" ai sensi dell'articolo 4, punto 4), del GDPR. Gli AISP potrebbero ad esempio avvalersi del trattamento automatizzato dei dati personali al fine di valutare taluni aspetti personali relativi a una persona fisica. A seconda delle specificità del servizio, potrebbe essere valutata la situazione finanziaria personale dell'interessato. I servizi di informazione sui conti, che sono prestati su richiesta dell'utente, possono comportare una valutazione approfondita dei dati personali relativi ai conti di pagamento.

82. Il titolare del trattamento deve inoltre essere trasparente nei confronti dell'interessato in merito all'esistenza di un processo decisionale automatizzato, compresa la profilazione. In tali casi il titolare del trattamento deve fornire informazioni significative sulla logica utilizzata, nonché sull'importanza e sulle conseguenze previste di tale trattamento per l'interessato (articolo 13, paragrafo 2, lettera f), articolo 14, paragrafo 2, lettera g), e considerando 60)[43]. Analogamente, a norma dell'articolo 15 del GDPR, l'interessato ha il diritto di chiedere e ottenere dal titolare del trattamento informazioni in merito all'esistenza di un processo decisionale automatizzato, compresa la profilazione, alla logica utilizzata e alle conseguenze per l'interessato e, in determinate

indipendentemente dal modo in cui utilizzano il servizio. Il fatto che l'interessato possa modificare manualmente le impostazioni sulla privacy tramite un apposito dashboard può inoltre facilitare la personalizzazione della dichiarazione/informativa sulla privacy, che sarà in grado di rispecchiare solo i tipi di trattamento che si verificano per quel particolare interessato.

40 Cfr. ad esempio il "consenso esplicito" di cui all'articolo 67, paragrafo 2, lettera a), della PSD2.

41 Cfr. anche EBA/OP/2020/10, punto 45.

42 Articolo 5, paragrafo 2, e articolo 24 del GDPR.

43 Linee guida sulla trasparenza ai sensi del regolamento 2016/679, WP 260 rev.01, approvate dall'EDPB.

circostanze, ha il diritto di opporsi alla profilazione, indipendentemente dal fatto che abbia luogo un processo decisionale totalmente automatizzato relativo alle persone fisiche[44].

83. In questo contesto rileva inoltre il diritto dell'interessato di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona, come previsto dall'articolo 22 del GDPR. Tale norma prevede inoltre, in determinate circostanze, la necessità che il titolare del trattamento attui misure appropriate per tutelare i diritti dell'interessato, che dovrebbero comprendere la specifica informazione all'interessato e il diritto di ottenere l'intervento umano nel processo decisionale, di esprimere la propria opinione e di contestare la decisione. Come indicato anche al considerando 71 del GDPR, ciò implica, tra l'altro, che gli interessati hanno il diritto di non essere sottoposti a una decisione, come il rifiuto automatico di una domanda di credito online, senza alcun intervento umano[45].

84. Il processo decisionale automatizzato, compresa la profilazione, che comporta l'uso di categorie particolari di dati personali è consentito soltanto se sono soddisfatte le condizioni cumulative di cui all'articolo 22, paragrafo 4, del GDPR:

- è applicabile un'esenzione di cui all'articolo 22, paragrafo 2;
- si applica l'articolo 9, paragrafo 2, lettere a) o g), del GDPR. In entrambi i casi il titolare del trattamento deve adottare misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato[46].

85. Come indicato nelle suddette linee guida, dovrebbero essere rispettati anche i requisiti per l'ulteriore trattamento. I chiarimenti e le indicazioni riguardanti il processo decisionale automatizzato relativo alle persone fisiche e la profilazione forniti dal gruppo di lavoro Articolo 29 nelle linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679, approvate dall'EDPB, sono pienamente pertinenti nel contesto dei servizi di pagamento e dovrebbero pertanto essere presi in debita considerazione.

Per il Comitato europeo per la protezione dei dati

La presidente

(Andrea Jelinek)

[44] Gruppo di lavoro Articolo 29, linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679, WP 251 rev.01.

[45] Considerando 71 del GDPR.

[46] Gruppo di lavoro Articolo 29, linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679, WP 251 rev.01, pag. 24.