CSA Italy

Principi di sicurezza applicabili ai Cloud Computing Services: GDPR, Direttiva NIS e PSD2 a confronto

---

Aprile 2020

Foto di copertina: Autore Raphaël Biscaldi (https://unsplash.com/)

Introduzione

La protezione dei dati personali e, ancor più in generale, la sicurezza informatica sono diventati negli ultimi anni temi di importanza primaria sia a livello nazionale che a livello sovranazionale. Ciò è testimoniato dall'adozione (nel 2016) e successiva applicazione (nel 2018) di due normative comunitarie che hanno ridisegnato la cornice di riferimento per la protezione dei dati e per la sicurezza dei sistemi informativi: il Regolamento Generale sulla Protezione dei dati personali ("Regolamento" o "GDPR")[1] e la Direttiva 2016/1148 sulla sicurezza delle reti e dei sistemi informativi, meglio nota come Direttiva NIS (*Network and Information Security*).[2] In questo quadro normativo si inserisce anche la Direttiva 2015/2366/(UE)[3] sui servizi di pagamento prestati nel mercato interno europeo ("PSD2") che ha introdotto significative novità nel mondo dei pagamenti digitali.

I fornitori dei servizi cloud ("cloud service providers" o "CSPs") sono quindi stati "investiti" dal susseguirsi di novità normative e dal sovrapporsi di numerosi obblighi derivanti dalla spesso simultanea applicazione del GDPR, della Direttiva NIS e, talvolta, anche della PSD2. La sovrapposizione delle disposizioni prescritte da normative differenti può ingenerare confusione nella gestione degli obblighi da queste imposti. Fare chiarezza in questo contesto di incertezza risulta di essenziale importanza non solo per permettere una corretta gestione dei vari adempimenti ma anche per permettere ai destinatari di tali obblighi di sfruttare tali sovrapposizioni al fine di ottimizzare, invece che moltiplicare, i propri sforzi applicativi.

La presente ricerca si propone quindi di analizzare le prescrizioni contenute nel GDPR e nella Direttiva NIS in materia di sicurezza al fine di individuare: (1) le misure tecniche e organizzative che i fornitori di servizi cloud sono tenuti ad applicare e gli obblighi di notifica previsti dal Regolamento e dalla Direttiva; (2) le sovrapposizioni e, al contempo, (3) le differenze tra le prescrizioni in esame nel loro contenuto, nei loro presupposti applicativi, nei criteri e nei rischi sulla base dei quali l'adeguatezza delle misure di sicurezza deve essere valutata. Questa analisi sarà inoltre completata dall'esame dei corrispettivi obblighi imposti dalla PSD2.

[1] 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).

[2] Direttiva (UE) 2016/1148 del Parlamento Europeo e del Consiglio del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

[3] Direttiva (UE) 2015/2366 del Parlamento Europeo e del Consiglio del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE.

Indice

Si ringrazia

Coordinatori del Gruppo di Lavoro "Legal & Privacy in the Cloud"

Isabella Oldani, Valerio Vertua

Autori

Isabella Oldani

Marco Tullio Giordano

Massimo Simbula

Review

Comitato Scientifico CSA Italy, Prof. Avv. Giovanni Ziccardi

Consiglio Direttivo CSA Italy

I principi e le misure di sicurezza applicabili ai Cloud Service Providers: l'approccio del GDPR

1.1 Misure tecniche e organizzative previste dal GDPR

Il GDPR, adottato il 27 aprile 2016 e divenuto applicabile il 25 maggio 2018, mira a **rafforzare e ad adattare all'era digitale il diritto alla protezione dei dati personali**, nonché agevolare le attività economiche, **assicurando** una libera – ma corretta – **circolazione dei dati personali** tra gli Stati membri. La sicurezza del trattamento dei dati costituisce uno dei principi chiave del Regolamento.

In tema di obbligo di implementazione di adeguate misure tecniche ed organizzative da parte del Titolare del trattamento, dunque, le disposizioni da considerare sono innanzitutto quelle contenute nella sezione "Obblighi Generali" del Capo IV del Regolamento, nello specifico quelle contenute negli articoli **24** commi 1 e 2 e **25**.

La previsione specificamente contenuta nell'art. 24 del GDPR richiede infatti che il Titolare metta in atto "**misure tecniche ed organizzative" adeguate per garantire, ed essere in grado di dimostrare, che il trattamento sia effettuato conformemente al Regolamento**, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche. La norma impone quindi l'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione dell'intero Regolamento. È evidente che si è dinanzi ad una norma dal contenuto estremamente ampio, che presuppone una vera e propria "portata globale dell'obbligo di responsabilità", che contempla quindi, nello specifico:

- l'obbligo di implementare misure che rendano ogni trattamento effettuato come conforme alle previsioni normative di settore;
- l'obbligo che le misure adottate forniscano garanzia di tale conformità;
- l'obbligo di fondare la scelta delle misure adottate su una preventiva analisi dei rischi;
- l'obbligo che tale conformità sia anche immediatamente dimostrabile, di fatto imponendo un vero e proprio obbligo di rendicontazione.

Per quanto riguarda l'attività richiesta al Titolare del trattamento, gli obblighi di valutazione delle misure e di garanzia della protezione dei dati trovano la loro origine fin dalla fase della progettazione e protezione per impostazione predefinita,[4] così come disposto dall'art. 25[5] GDPR.

[4] I principi di *privacy by design* e *privacy by default* impongono ai titolari ed ai responsabili del trattamento l'obbligo di avviare un progetto prevedendo, fin da subito ed in fase di programmazione, eventuali rischi che potrebbero

L'attività di adeguamento e costante intervento e rendicontazione del Titolare e del Responsabile del trattamento, tuttavia, prosegue anche successivamente alla preliminare fase di progettazione e, nello specifico, è prevista quale costante attenzione dei soggetti preposti alla sicurezza dei dati durante tutta l'esecuzione del trattamento. L'art. 32, che apre la Sezione Seconda del Regolamento, è specificamente dedicato a dettagliare i principi in tema di "*Sicurezza del trattamento*".

Le misure di sicurezza, quindi, devono essere adeguate, imponendo non una obbligazione di risultato, bensì una c.d. obbligazione di mezzi, in modo che le misure siano ragionevolmente soddisfacenti alla luce delle conoscenze e delle prassi.

Per fare questo essi dovranno tenere debitamente conto dell'attuale stato dell'arte (della tecnologica disponibile, dei sistemi informatici, etc.), dei costi di attuazione, della natura dei dati e dei meccanismi adottati, del campo di applicazione, del contesto e delle finalità del trattamento dei dati, oltre che del rischio per i diritti e le libertà delle persone fisiche, che può essere più o meno probabile e più o meno alto a seconda di ciascun diverso contesto.

Più nello specifico, le misure che il titolare o il responsabile del trattamento dei dati devono concretamente adottare sono, come stabilito dall'art. 32(1):

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
- una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Per quanto concerne ad esempio la **pseudonimizzazione**, questa deve essere intesa come un particolare trattamento dei dati personali realizzato in modo tale che i dati stessi non possano più essere attribuiti direttamente ed automaticamente ad un interessato specifico. Infatti, i trattamenti si intendono pseudonimizzati quando tali dati potranno essere ricondotti all'interessato cui si riferiscono solo attraverso l'impiego di altre informazioni aggiuntive, che dovranno essere, a tal fine, conservate separatamente e con

---

intervenire in corso d'opera, al fine di garantire in maniera preventiva la tutela dei dati personali e, di conseguenza, intervenire a priori nella scelta degli strumenti di sicurezza più idonei a garantire i diritti degli interessati.

[5] L'art. 25 del GDPR prevede infatti che "*il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati*" (comma 1), nonché che "*il titolare del trattamento mette 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*" (comma 2). Inoltre, il medesimo articolo specifica che "*tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica*".

l'impiego di precauzioni tecniche e organizzative adeguate[6]. La finalità ultima è difatti quella di garantire che i dati personali non possano essere attribuiti ad una persona fisica identificata o identificabile.

La **cifratura** dei dati personali, invece, è quella tecnica più definitiva, volta a rendere i dati personali inintelligibili a chiunque non sia autorizzato ad accedervi e consiste, più specificamente, nella "*conversione delle informazioni originali in una sequenza apparentemente causale di numeri, lettere e segni speciali, tale per cui il risultato sia irreversibile*" attraverso l'utilizzo di meccanismi che normalmente prevedono l'impiego di algoritmi di crittografia.

Per **riservatezza** si intende l'assenza di divulgazioni o accessi ai dati non autorizzati e si garantisce attraverso una attenta gestione della sicurezza fisica e logica, in modo tale da mitigare i rischi connessi all'accesso o all'uso delle informazioni in forma non autorizzata. Strumenti che garantiscono il rispetto del principio di riservatezza dei dati sono una corretta impostazione dei diritti di accesso al dato ed una politica di access-control efficace, nonché una solida attenzione al perimetro di sicurezza delle infrastrutture informatiche.

Per **integrità** dei dati si intende la garanzia che l'informazione non subisca modifiche o cancellazioni a seguito di errori o di azioni volontarie, ma anche a seguito di malfunzionamenti o danni dei sistemi tecnologici.

Per **disponibilità** dei dati si intende la salvaguardia del patrimonio informativo nella garanzia di accesso, usabilità e confidenzialità dei dati. Da un punto di vista di gestione della sicurezza significa ridurre a livelli accettabili i rischi connessi all'accesso alle informazioni (intrusioni, furto di dati, ecc.). La disponibilità si garantisce implementando soluzioni di back up che escludano la possibilità di perdita dei dati e soluzioni tecnologiche che li rendano sempre a disposizione.

Per **resilienza** dei dati si intende la loro capacità che essi rimangano disponibili per le applicazioni e gli utenti anche se si verifica un malfunzionamento del sistema su cui essi si trovavano in origine.

La norma attribuisce rilievo anche al concetto di ***disaster recovery***, che consiste nella capacità di reagire in modo efficace e tempestivo ad eventuali criticità dovute ad incidenti fisici o tecnici, allo scopo di ripristinare la disponibilità e l'accesso dei dati personali oggetto di trattamento.[7] A tale riguardo, sarà quindi importante per i titolari predisporre un programma specifico attraverso cui analizzare innanzitutto i rischi che potrebbero andare a colpire il sistema informatico; prevedere poi le adeguate misure da adottare per minimizzarli; ed infine predisporre un piano di emergenza che permetta di attuare un sistema alternativo di elaborazione dei dati da utilizzare in attesa della completa riattivazione.

---

[6] la definizione datane direttamente dal GDPR, all'art. 4 n. 5, è la seguente: "*il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile*".

[7] Il c.d. Disaster Recovery Plan fa parte del più ampio Business Continuity Plan: mentre il primo documento serve all'azienda per affrontare un evento in grado di compromettere la funzionalità tecnologica di dati e sistemi critici (ad es. un guasto, un attacco hacker etc.), il secondo tiene conto di tutti gli eventi in grado di avere un impatto economico, normativo, legale, finanziario o reputazionale sull'azienda, sia a causa di un'interruzione del funzionamento del reparto IT che, ad es., della mancanza di infrastrutture o di risorse umane.

Per la prima volta, con il Regolamento, viene prescritto l'obbligo, ulteriore rispetto al dotarsi delle misure di sicurezza volte a garantire i principi fin qui espressi, di verificare che tali misure siano idonee all'obiettivo che il titolare ed il responsabile devono prefiggersi.[8]

Ribadendo che, come previsto dall'art. 32(1) sopra richiamato, le misure di sicurezza dovranno essere tali da "garantire un livello di sicurezza adeguato al rischio" creato dal trattamento, l'**elencazione** delle misure fatta dal GDPR deve essere necessariamente considerata **esemplificativa e non esaustiva** e, in questo senso, aperta all'individuazione di altre diverse possibili misure ideate in base al contesto concreto in cui vengono poste in essere.

In questo senso, il GDPR si differenzia notevolmente dalle previgenti normative sulla protezione dei dati personali. Le normative in materia di protezione dei dati personali in vigore nelle giurisdizioni europee prima dell'entrata in vigore del GDPR[9], infatti, si limitavano a prevedere, in capo ai soggetti attivi del trattamento, un generico obbligo di diligenza che, in tema di messa in sicurezza del dato, si concretizzava nell'implementazione di una lista di quelle che venivano definite "misure minime" di sicurezza. Erano generalmente previste, inoltre, alcune ulteriori ed aggiuntive "misure idonee", da adottare in base alla specifica attività svolta nel corso del trattamento ed alla natura particolare dei dati conferiti dagli interessati. Differentemente, come visto sopra, il GDPR prevede una serie di obblighi positivi, anche di natura tecnica e procedimentale, tali per cui si rende necessario che il titolare ed il responsabile del trattamento coltivino oggi non solo conoscenze giuridiche e organizzative, ma si preoccupino specificamente anche di curare l'implementazione di altrettante soluzioni informatiche.

Il GDPR, del resto, pone con forza l'accento sulla c.d. ***accountability*** di titolari e responsabili – che consiste nell'adozione di **comportamenti proattivi** e tali da dimostrare la concreta implementazione di misure, effettive e tecnologicamente avanzate, finalizzate ad assicurare l'applicazione delle disposizioni regolamentari. Si tratta di una grande novità per la protezione dei dati, in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali – nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel testo normativo. Rispetto agli evidenti limiti riscontrabili nelle normative nazionali dei singoli Stati europei, tra cui il Codice della privacy italiano – dove tali misure si concretizzavano in un elenco dettagliato e uguale per tutti i soggetti coinvolti, a prescindere dall'attività svolta e dalle relative sensibilità in tema di trattamento di dati

[8] Un esempio di tali misure è la pianificazione di periodici penetration test che testino la resistenza dei sistemi ad eventuali attacchi esterni. Ugualmente, la verifica della funzionalità delle misure di backup è idonea a garantire la loro efficacia in caso di necessità. Per la conformità al GDPR, i penetration test sono fondamentali. Forniscono un controllo finale per assicurarsi che tutti i controlli di sicurezza siano stati implementati e funzionino correttamente. Possono anche essere utilizzati nelle prime fasi di sviluppo di nuovi sistemi di elaborazione per identificare potenziali rischi alla sicurezza dei dati personali.

[9] Tutte direttamente discendenti dalla Direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, e dalla Direttiva 2002/58/CE (anche conosciuta con il nome di "*ePrivacy*"), poi modificata dalla direttiva 2009/136/CE, 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).

personali e sensibili – il GDPR cambia totalmente approccio, lasciando al titolare ed al responsabile del trattamento ampio margine di libertà di scelta in funzione della realtà produttiva nella quale opera.

Inoltre, è opportuno richiamare l'attenzione sulla possibilità, prevista dall'art. 32, dell'utilizzo di specifici **codici di condotta** o **meccanismi di certificazione** che consentano di documentare l'idoneità delle misure di sicurezza adottate. In ambito cloud, si segnalano i seguenti codici di condotta: il Codice di Condotta di Cloud Security Alliance,[10] CISPE Code of Conduct,[11] EU Cloud Code of Conduct.[12] Questi codici di condotta non sono ancora stati formalmente approvati e riconosciuti dalle rispettive autorità di controllo, ai sensi dell'articolo 40(5) del GDPR, quali strumenti di certificazione della conformità al Regolamento, ma offrono comunque una guida efficiente ai fini della compliance e permettono ai CSPs di mostrare in modo chiaro e trasparente, sia ai propri clienti che alle autorità, il livello di protezione da questi garantito.

L'articolo 33 GDPR, inoltre, impone al titolare del trattamento l'**obbligo di notifica** all'autorità di controllo nel caso di **violazione di dati personali** (o "*data breach*")[13] quando da questa possa derivare un **rischio per i diritti e le libertà delle persone** (Articolo 33 GDPR), come la limitazione di alcuni diritti, il furto d'identità, una perdita finanziaria o un danno alla reputazione. Il titolare dovrà procedere alla notifica senza ingiustificato ritardo e, ove possibile, **entro 72 ore** da quando ne è venuto a conoscenza. Inoltre, nei casi in cui la violazione dei dati personali sia suscettibile di presentare un **rischio *elevato* per i diritti e le libertà degli interessati**, il Titolare dovrà **comunicare** la violazione all'interessato qualora questa possa "presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (Articolo 34 GDPR).

Il rispetto del principio di sicurezza assume primaria importanza ogni qual volta l'attività di trattamento viene **esternalizzata** a soggetti terzi, specialmente se tali soggetti sono fornitori di servizi cloud. Il ricorso a servizi cloud comporta infatti il rischio di perdita di controllo sui dati "ceduti" al fornitore. Il rischio di perdita di controllo sui dati deriva dalle difficoltà, se non impossibilità, per il titolare di controllare il sistema informatico impiegato dal cloud provider, difficoltà accentuate dal fatto che spesso i server in cui i dati vengono trattati sono localizzati al di fuori dello Spazio Economico Europeo (si veda sul punto il paragrafo 2.2).

Al fine di evitare che l'esternalizzazione delle attività di trattamento a soggetti terzi comporti una diminuzione degli standard di sicurezza imposti dal Regolamento, il GDPR, specificamente **l'art. 28** disciplinante la figura del "responsabile del trattamento", impone al titolare di ricorrere esclusivamente a fornitori "*che presentino **garanzie sufficienti** per mettere in atto misure tecniche e organizzative adeguate*", in modo da garantire il rispetto del GDPR e la tutela dei diritti degli interessati.[14] È quindi responsabilità del titolare avvalersi di fornitori di servizi cloud che dimostrino di essere in grado di rispettare i requisiti imposti dal Regolamento.

---

[10] https://cloudsecurityalliance.org/artifacts/cloud-security-alliance-code-of-conduct-for-gdpr-compliance/
[11] https://cispe.cloud/code-of-conduct/
[12] https://eucoc.cloud/en/contact/request-the-eu-cloud-code-of-conduct.html
[13] Articolo 4 n.12 GDPR: "'violazione dei dati personali': la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".
[14] Articolo 28(1) GDPR.

Lo strumento predisposto dal GDPR per far sì che il titolare possa mantenere il controllo sui dati trattati per suo conto da soggetti terzi è rappresentato dal contratto di cui al medesimo articolo 28 GDPR (denominato "***data processing agreement***" e solitamente abbreviato in "DPA"). Il responsabile del trattamento deve, infatti, essere vincolato al titolare del trattamento da un contratto che definisca "*la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento*".[15]

Non a caso, tra i vari obblighi a carico del responsabile che devono essere inclusi nel contratto vi è anche l'obbligo di adottare le misure tecniche ed organizzative previste dall'articolo 32 GDPR.[16] Alle misure di sicurezza è infatti spesso dedicato un apposito allegato al DPA. Il contratto deve inoltre prevedere, sempre a carico del responsabile, l'**obbligo di assistere il titolare** nell'adempimento di varie disposizioni del Regolamento che presuppongono la necessaria collaborazione da parte del responsabile, tra cui le disposizioni agli articoli 32, 33 e 34 GDPR.[17] La collaborazione del responsabile è senza dubbio essenziale nel caso in cui si verifichi una violazione dei dati personali. Il titolare del trattamento non potrebbe infatti notificare la violazione all'Autorità Garante, né comunicarla agli interessati e non potrebbe nemmeno valutare la necessità/opportunità di procedere alla suddetta notifica o comunicazione se non fosse informato dal responsabile del trattamento sulle circostanze della violazione in questione.

Per garantire che le misure di sicurezza predisposte dal responsabile siano rispettate nel corso di tutta la durata del rapporto contrattuale tra il titolare e il responsabile, il responsabile deve inoltre impegnarsi a consentire al titolare di svolgere tutte le attività di revisione, incluse le ispezioni e gli audit tecnici, che si rendano necessari per verificare il rispetto degli obblighi contrattuali.[18]

1.2 I principi di sicurezza in relazione al trasferimento dei dati a paesi terzi

Come anticipato, l'utilizzo dei servizi *cloud* comporta specifici rischi in materia di sicurezza e, in particolare, il rischio di **perdita di accesso e controllo** dei dati "ceduti" al fornitore di servizi *cloud*. La capacità del titolare di verificare la corretta gestione dei dati è ancor più affievolita se si considera che spesso l'utilizzo dei servizi cloud comporta anche il trasferimento di dati in **server** localizzati al di fuori dell'Unione Europea, o meglio, **al di fuori dello Spazio Economico Europeo**. In questo contesto, il titolare potrebbe perfino non essere in grado di verificare l'esatta localizzazione dei dati. Il livello di rischio aumenta se si considera che i paesi terzi verso cui i dati vengono trasferiti spesso garantiscono un livello di protezione inferiore a quello imposto a livello UE e se si considera che i dati localizzati in un data center di un paese terzo potrebbero essere oggetto di richieste di accesso da parte delle autorità pubbliche del paese in questione.

Il capo V del GDPR prescrive un'apposita disciplina per il trasferimento di dati verso paesi terzi a cui è assimilato il trasferimento verso organizzazioni internazionali. In particolare, l'articolo 44 GDPR prescrive, come principio generale, che *"[q]ualunque trasferimento di dati personali oggetto di un trattamento o*

[15] Articolo 28(3) GDPR.
[16] Articolo 28(3)(c) GDPR.
[17] Articolo 28(3)(f) GDPR.
[18] Articolo 28(3)(h) GDPR.

destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale … ha luogo soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni di cui" al capo V GDPR. Le disposizioni del capo V sono volte a garantire che il **livello di protezione prescritto dal Regolamento non sia pregiudicato per effetto del trasferimento** e, quindi, che il **livello di protezione disposto dal Regolamento, anche in termini di sicurezza, "viaggi" con i dati**.[19]

In primo luogo, il Regolamento dispone che il trasferimento di dati all'estero è consentito sulla base di una **decisione di adeguatezza**,[20] ovvero una decisione con la quale la Commissione Europea ha stabilito che il paese terzo[21] (o l'organizzazione internazionale) in questione garantisce un livello di protezione adeguato, ovvero, un livello di protezione "essenzialmente equivalente"[22] a quello garantito a livello UE. Questa decisione ha l'effetto di consentire la libera circolazione dei dati senza che siano necessarie ulteriori garanzie o autorizzazioni.

Il Gruppo di Lavoro Articolo 29 per la Protezione dei Dati ("Gruppo di lavoro Articolo 29") ha individuato una serie di criteri sulla base dei quali l'adeguatezza del livello di protezione offerto da un paese terzo deve essere valutata.[23] In particolare, il Gruppo di lavoro Articolo 29 ha selezionato alcuni principi generali di protezione dei dati personali che il sistema di un paese terzo deve prevedere per potere essere considerato "adeguato". Tra questi principi figura anche il "principio della sicurezza e della riservatezza" ai sensi del quale "*[q]ualsiasi organismo incaricato del trattamento dei dati dovrebbe assicurare che questi siano trattati in maniera da garantire un'**adeguata sicurezza dei dati personali**, compresa la protezione, mediante **misure tecniche e organizzative adeguate**, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali. Il livello di sicurezza dovrebbe tenere in considerazione lo **stato dell'arte e i relativi costi***".[24] È quindi evidente che affinché un paese terzo possa essere considerato adeguato, il suo sistema normativo deve includere dei principi di sicurezza analoghi a quelli previsti dal GDPR e, in particolare, dall'Articolo 32 GDPR.

In mancanza di una decisione di adeguatezza, il Regolamento offre altri meccanismi a cui è possibile ricorrere per trasferire i dati verso paesi terzi. A norma dell'Articolo 46 GDPR, infatti, in mancanza di una decisione di adeguatezza, il titolare o il responsabile del trattamento possono ricorrere a strumenti alternativi che offrono "**garanzie adeguate**".

---

[19] Commissione Europea, Comunicazione della Commissione al Parlamento Europeo e al Consiglio, Scambio e protezione dei dati personali in un mondo globalizzato, Bruxelles, 10.1.2017, COM(2017) 7 final, 4.
[20] Articolo 45 GDPR.
[21] Oppure "un territorio o uno o più settori specifici all'interno del paese terzo".
[22] Sentenza della Corte di giustizia dell'Unione europea del 6 ottobre 2015, *Maximillian Schrems/Data Protection Commissioner*, C-362/14, ECLI:EU:C:2015:650. Si veda inoltre il considerando 104 del GDPR: "Il paese terzo dovrebbe offrire garanzie di un adeguato livello di protezione sostanzialmente equivalente a quello assicurato all'interno dell'Unione, segnatamente quando i dati personali sono trattati in uno o più settori specifici. In particolare, il paese terzo dovrebbe assicurare un effettivo controllo indipendente della protezione dei dati e dovrebbe prevedere meccanismi di cooperazione con autorità di protezione dei dati degli Stati membri e agli interessati dovrebbero essere riconosciuti diritti effettivi e azionabili e un mezzo di ricorso effettivo in sede amministrativa e giudiziale".
[23] Gruppo di Lavoro Articolo 29 per la Protezione dei Dati, Criteri di riferimento per l'adeguatezza, adottati il 28 novembre 2018, versione emendata e adottata il 6 febbraio 2018 (WP254 rev.01).
[24] WP254 rev.01, 6.

Tra questi strumenti, occorre ricordare le clausole contrattuali tipo ("*standard contractual clauses*", "SCCs")[25] e le norme vincolanti d'impresa ("*Binding Corporate Rules*", "BCRs").[26]

Le **clausole contrattuali tipo** sono strumenti contrattuali attraverso i quali l'esportatore (in qualità di titolare del trattamento) vincola l'importatore (in qualità di titolare o responsabile del trattamento) al rispetto dei principi previsti dalla normativa UE. Questa garanzia si estende anche alle misure di sicurezza che devono essere implementate dall'importatore. Le clausole contrattuali infatti impongono all'importatore di attuare le misure tecniche e organizzative necessarie a proteggere i dati e a garantire un livello di sicurezza adeguato ai rischi a cui i dati sono esposti.[27] In particolare, "[*n]el contratto le parti devono prevedere le* ***misure tecniche e organizzative*** *necessarie che, tenuto conto della normativa sulla protezione dei dati, della più recente tecnologia e dei costi di attuazione,* ***sono necessarie a garantire la protezione dei dati personali*** *dalla distruzione accidentale o illecita, dalla perdita accidentale, dall'alterazione, dalla diffusione o dall'accesso non autorizzati, o da qualsiasi altra forma illecita di trattamento di dati personali*".[28] L'importatore inoltre dichiara e garantisce che, a richiesta dell'esportatore, sottoporrà i propri impianti o servizi di trattamento al controllo dell'esportatore.[29]

Le **norme vincolanti d'impresa** permettono il trasferimento di dati tra i membri di un gruppo imprenditoriale o di un gruppo di imprese che svolgono attività economica comune. L'articolo 47 GDPR individua una serie di requisiti che le BCRs devono soddisfare per potere essere approvate dall'autorità di controllo competente. Tra questi requisiti sono incluse anche "*le misure a garanzia della sicurezza dei dati*".[30] Le BCR devono infatti includere esplicitamente una descrizione dei principi di protezione dei dati, tra cui il principio di sicurezza di cui all'articolo 5(f) e 32 del Regolamento che comprende anche "*l'obbligo di stipulare contratti con tutti i subcontraenti/responsabili del trattamento interni ed esterni, che comprendano tutti i requisiti di cui all'articolo 28, paragrafo 3, del regolamento nonché l'obbligo di segnalare senza ingiustificato ritardo eventuali violazioni di dati personali … e, se la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, agli interessati*".[31]

---

[25] Articolo 46(2)(c) e (d) GDPR.

[26] Articolo 47 GDPR.

[27] Appendice 2 alle clausole contrattuali tipo, Decisione della Commissione del 15 giugno 2001 relativa alle clausole contrattuali tipo per il trasferimento di dati a carattere personale verso paesi terzi a norma della direttiva 95/46/CE, L 181/19 ("SCCs 2001"); Clausola II(a) e allegato A alle clausole contrattuali tipo, Decisione della Commissione del 27 dicembre 2004 che modifica la decisione 2001/497/CE per quanto riguarda l'introduzione di un insieme alternativo di clausole contrattuali tipo per il trasferimento di dati personali a paesi terzi, L 385/74 ("SCCs 2004"); Clausola 4(c)(d)(e), clausola 5(c) e appendice 2 alle clausole contrattuali tipo, Decisione della Commissione del 5 febbraio 2010 relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento stabiliti in paesi terzi a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, L 39/5 ("SCCs 2010").

[28] Considerando 12, Decisione della Commissione del 5 febbraio 2010 relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento stabiliti in paesi terzi a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, L 39/5 (enfasi aggiunta).

[29] Clausola 5(d) SCCs 2001; clausola II(g) SCCs 2004; clausola 5(f) SCCs 2010.

[30] Articolo 47(2)(d) GDPR.

[31] Criterio di approvazione 6.1.1. Gruppo di Lavoro Articolo 29 per la Protezione dei Dati, Documento di lavoro che istituisce una tabella degli elementi e dei principi che devono figurare nelle norme vincolanti d'impresa, adottato il 28 novembre 2017, versione emendata e adottata il 6 febbraio 2018, WP 256 rev.01. Si veda anche criterio 6.1 Gruppo di

È evidente da quanto sopra esposto che la sicurezza dei dati è uno dei principi fondamentali che il titolare e il responsabile sono chiamati a garantire e che il GDPR cerca di preservare **indipendentemente dalla localizzazione dei dati**. Al fine di limitare l'esposizione ai rischi che il trasferimento dei dati porta con sé, vari cloud providers, tra cui Google,[32] Amazon Web Services[33] e Microsoft[34] permettono ai propri clienti di selezionare i servers in cui localizzare i dati, tra cui servers localizzati nello Spazio Economico Europeo. Tale facoltà è però spesso riservata ad alcuni servizi o ad alcune tipologie di dati.

Invece di limitare il trasferimento *tout court*, si potrebbe considerare la possibilità di **anonimizzare** i dati prima di procedere al loro trasferimento. Ai sensi del considerando 26 del GDPR infatti, i principi di protezione stabiliti dal GDPR non dovrebbero applicarsi ai dati personali che sono stati resi sufficientemente anonimi da non consentire più l'identificazione del soggetto a cui i dati si riferiscono. L'anonimizzazione dei dati permetterebbe quindi non solo di ridurre al minimo i rischi a cui i dati sono esposti per effetto del trasferimento ma anche di procedere al trasferimento senza dover implementare le misure di cui al Capo V del Regolamento. Al contempo, occorre ricordare che il processo di anonimizzazione dei dati rientra all'interno della definizione di "trattamento" di cui all'Articolo 4 GDPR e necessita pertanto, come tutte le attività di trattamento, di una idonea base giuridica.[35]

Un'altra soluzione che potrebbe essere implementata per limitare i rischi a cui i dati sono esposti nel momento in cui vengono "ceduti" a fornitori cloud al di fuori dello Spazio Economico Europeo consiste nel **cifrare** i dati prima che questi vengano trasferiti ai servizi cloud. I dati possono essere cifrati dallo stesso titolare/responsabile prima che questi vengano inviati al sistema cloud oppure da "intermediari" che cifrano i dati delle aziende prima che questi vengano localizzati sul cloud. Tali intermediari si pongono a metà strada tra le aziende e i loro fornitori di servizi cloud.

Per esempio, Veolia Environment, un'azienda francese di servizio pubblico, si è affidata ad Atos per la cifratura dei propri dati prima del loro trasferimento nel cloud di Google. Altre società europee, tra cui Thales e SAP, offrono alle aziende la possibilità di proteggere il loro patrimonio prima che questo venga

---

Lavoro Articolo 29 per la Protezione dei Dati, Documento di lavoro che istituisce una tabella degli elementi e dei principi che devono figurare nelle norme vincolanti d'impresa, adottato il 28 novembre 2017, versione emendata e adottata il 6 febbraio 2018, WP 257 rev.01.

[32] Sezione 1.4, Google Cloud Platform Terms of Service, https://cloud.google.com/terms/: "Customer may select where certain Customer Data will be stored ('Data Location Selection'), and Google will store it there in accordance with the Service Specific Terms".

[33] Sezione 12.1, Amazon Web Services, GDPR Data Processing Addendum, https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf: "Customer may specify the location(s) where Customer Data will be processed within the AWS Network, including the EU (Dublin) Region, the EU (Frankfurt) Region, the EU (London) Region and the EU (Paris) Region (each a "Region"). Once Customer has made its choice, AWS will not transfer Customer Data from Customer's selected Region(s) except as necessary to provide the Services initiated by Customer, or as necessary to comply with the law or binding order of a governmental body".

[34] Si veda la sezione sulla "posizione dei dati della società a riposo" delle Condizioni per l'Utilizzo dei Servizi Online di Microsoft, 1 ottobre 2019, p.12, https://www.microsoft.com/en-us/licensing/product-licensing/products.

[35] Provvedimento del Garante sulla Protezione dei Dati Personali in tema di fatturazione elettronica, 20 dicembre 2018, doc. web n. 9069072, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9069072; Gruppo di Lavoro Articolo 29 per la Protezione dei Dati, parere 5/2014 sulle tecniche di anonimizzazione, WP216, adottato il 10 aprile 2014.

trasferito sul cloud. La cifratura dei dati prima del loro trasferimento ai servizi cloud, accompagnata da una corretta gestione della chiave crittografia, permetterebbe quindi alle aziende europee di sfruttare la tecnologia dei principali cloud providers senza cedere a questi il controllo sui propri dati.[36] Al contempo, occorre ricordare che il Gruppo di lavoro Articolo 29 ha chiarito che "[i]n un ambiente cloud, il **criptaggio** può contribuire in misura significativa alla riservatezza dei dati personali, se attuato correttamente, ***benché non li renda anonimi in modo irreversibile***".[37] Se i dati cifrati possono ricondurre al soggetto a cui i dati si riferiscono, tali dati dovranno quindi essere trattati nel rispetto dei principi previsti dal GDPR, incluse le disposizioni in materia di trasferimento dei dati personali.

[36] https://www.bloomberg.com/news/articles/2019-06-28/european-companies-look-to-build-their-own-walls-in-the-cloud.

[37] Gruppo di Lavoro Articolo 29 per la Protezione dei Dati, Parere 05/2012 sul cloud computing, adottato il 1° luglio 2012, WP196, paragrafo 3.4.3.3.

I principi e le misure di sicurezza applicabili ai Cloud Service Providers: l'approccio della Direttiva NIS

Negli ultimi decenni i servizi elettronici, le nuove tecnologie, i sistemi di informazione e le reti si sono stabilmente integrati nella nostra vita quotidiana. È ormai noto che incidenti intenzionali, che causano l'interruzione dei servizi informatici e delle infrastrutture critiche, costituiscono una grave minaccia per il loro funzionamento e, di conseguenza, per il funzionamento del mercato interno e dell'Unione. Questo rischio, combinato con il fatto che le contromisure esistenti in termini di strumenti e procedure di sicurezza non sembrano sufficientemente sviluppati nel territorio dell'Unione Europea, e certamente non comuni in tutti gli Stati membri, ha reso insindacabile la necessità di un approccio globale a livello comunitario, relativo alla sicurezza della rete e dei sistemi di informazione. La Direttiva NIS mira a rispondere a questa esigenza presentando "*le misure volte a raggiungere un* ***livello comune elevato di sicurezza delle reti e dei sistemi di informazione*** *nell'Unione al fine di migliorare il funzionamento del mercato interno*".

Pochi mesi dopo l'adozione del GDPR, infatti, il Parlamento dell'Unione Europea e il Consiglio hanno adottato la Direttiva NIS, relativa all'istituzione di misure per un livello comune elevato di sicurezza delle reti e dei sistemi di informazione in tutta l'Unione. Nel gennaio 2018 poi, la Commissione europea ha emanato un regolamento di applicazione ai sensi di tale Direttiva (c.d. regolamento di esecuzione).[38] La Direttiva NIS è stata recepita in Italia con il decreto legislativo n. 65 del 18 maggio 2018,[39] entrato in vigore il 24 giugno 2018. Essa mira a conseguire un livello di sicurezza comune ed elevato della rete e dei sistemi informativi nell'Unione. A tal fine, la Direttiva NIS ha introdotto nuovi e rilevanti obblighi in materia di sicurezza. Tra questi, l'adozione di **misure tecniche-organizzative adeguate e proporzionate** per la gestione dei rischi e per la riduzione dell'impatto di eventuali incidenti informatici a carico della sicurezza della rete e dei sistemi informativi, nonché l'**obbligo di notifica di eventuali incidenti informatici** al *Computer Security Incident Response Team* (CSIRT) e, per conoscenza, all'autorità competente NIS del proprio settore.

La Direttiva NIS mira a rafforzare la sicurezza informatica entro in confini dell'Unione Europea attraverso il raggiungimento di due obiettivi principali:

- migliorare la preparazione e le capacità di garantire la sicurezza informatica degli Stati membri dell'UE, chiedendo ad ognuno di essi di stabilire un quadro nazionale per la sicurezza della rete e dei sistemi di informazione (NIS) che preveda l'istituzione di CSIRT nazionali (*Computer Security Incident Response Team*: testualmente team di risposta agli incidenti di sicurezza informatica), punti di contatto nazionali (SPOC) e ulteriori altrettante autorità nazionali in materia di rete e sistemi di informazione, nonché di collaborare attraverso un gruppo di cooperazione comunitaria della rete CSIRT; e
- imporre nuovi obblighi di sicurezza e obblighi di segnalazione degli incidenti, nello specifico prevedendo:
  - un primo set di obblighi a carico dei soggetti considerati da ciascun Stato membro come gestori, in modo efficace, di una infrastruttura critica (**operatori di "servizi essenziali**", "operatori essenziali" o "OES") come servizi pubblici, trasporti, assistenza sanitaria e

[38] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2018.026.01.0048.01.ENG&toc=OJ%3AL%3A2018%3A026%3ATOC.
[39] https://www.csirt-ita.it/files/dlgs_18_maggio_2018_n65.pdf.

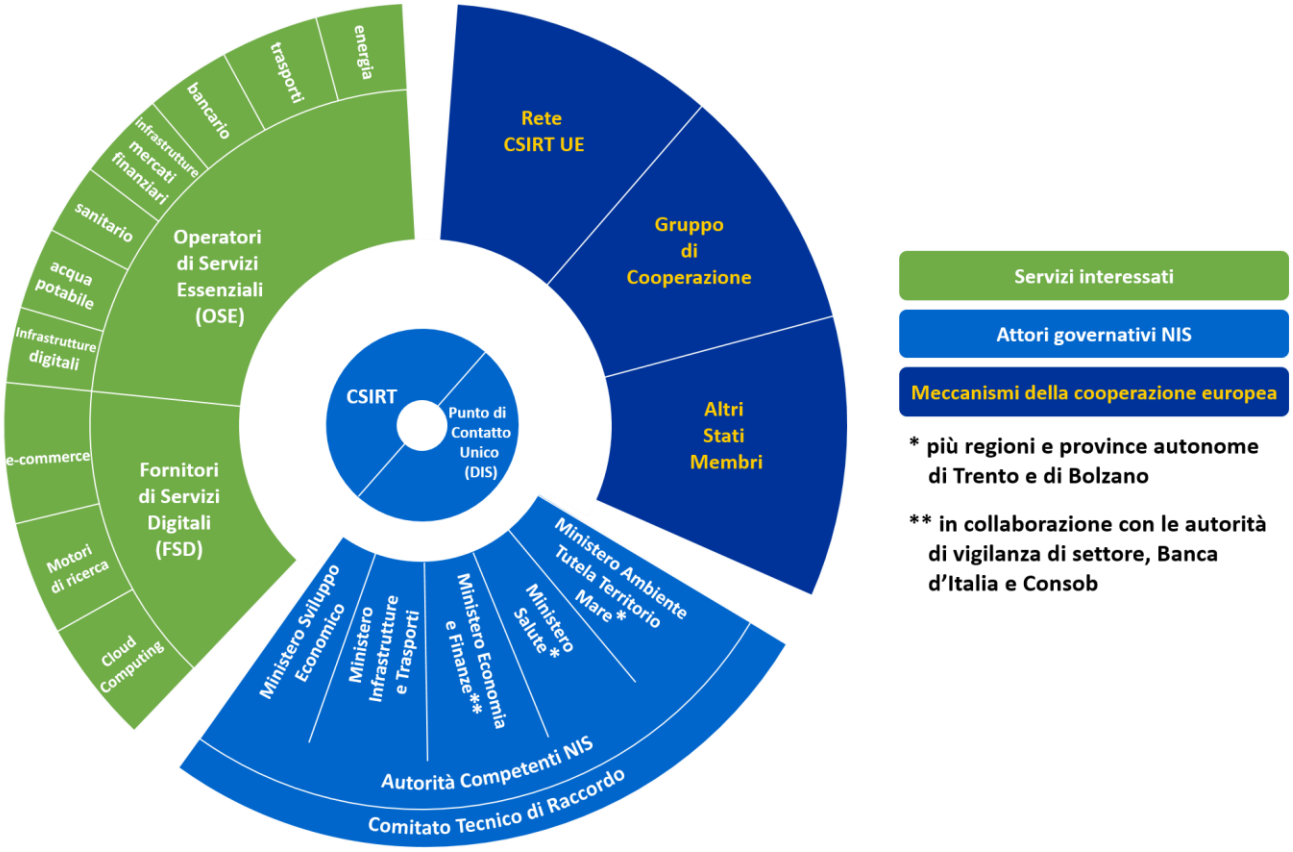
- con un intervento meno rigido, un ulteriore set di obblighi per quegli operatori classificati come "***fornitori di servizi digitali***" (DSP, acronimo di *Digital Service Providers*) ai sensi della Direttiva NIS.

I DSP sono **fornitori di servizi cloud**, marketplace e motori di ricerca. Considerando l'approccio più leggero, suggerito dalla Direttiva nei confronti di tali soggetti, gli Stati membri non possono imporre requisiti di sicurezza "aggiuntivi" o imporre ulteriori obblighi di notifica di incidenti ai DSP, fatte salve eventuali specifiche prescrizioni finalizzate a salvaguardare la sicurezza nazionale e mantenere la legge e l'ordine[40]. Nessun DSP può essere soggetto a una maggiore responsabilità derivante da obblighi di notifica[41].

La Direttiva si applica solo negli Stati membri che abbiano già provveduto ad implementare, di conseguenza, una specifica legislazione interna. Tutti gli Stati membri avrebbero dovuto recepirla a livello nazionale entro il 10 maggio 2018. Tuttavia, solo la Repubblica ceca, l'Estonia, la Germania, la Slovenia e il Regno Unito hanno rispettato il termine indicato e recepito integralmente i principi della NIS prima del termine indicato. Altri Stati la hanno recepita parzialmente e altri ancora sono arrivati in leggero ritardo. Tra essi, ad esempio, l'Italia ha terminato l'iter legislativo, come già indicato, soltanto alla fine del giugno 2018.

Il testo della Direttiva è composto da 27 articoli. Gli articoli da 1 a 6 ne definiscono il campo di applicazione e le principali definizioni, compreso un ulteriore chiarimento in merito all'identificazione degli operatori di servizi essenziali (dei quali viene fornita una definizione formale all'articolo 5), nonché al significato di ciò che deve essere considerato un "*significativo effetto negativo sul servizio*" (definizione contenuta nell'articolo 6). Gli articoli da 7 a 10 descrivono, invece, i *framework* nazionali che devono essere adottati da ciascuno Stato membro sulla sicurezza della rete e dei sistemi di informazione. Tali *framework* comprendono, tra l'altro, l'obbligo degli Stati membri di introdurre una strategia nazionale e di designare le autorità nazionali competenti (compresa l'indicazione di SPOC e CSIRT), nonché la creazione del gruppo comune di cooperazione. Il meccanismo di cooperazione è previsto nel capitolo III e più precisamente negli articoli da 11 a 13. Infine, gli articoli che chiudono il testo normativo (14 – 18) definiscono i requisiti di sicurezza e la procedura di notifica degli incidenti, rispettivamente, per gli operatori dei servizi essenziali e per i fornitori di servizi digitali e il processo di notifica volontaria è trattato negli articoli 19 e 20. Infine, gli articoli 21-27 includono le disposizioni finali della Direttiva.

[40] Articolo 16(10), Articolo 1(6) Direttiva NIS.
[41] Articolo 16(3) Direttiva NIS.



Fonte: https://www.csirt-ita.it/

Ai fini del presente contributo, risulta utile approfondire gli obblighi di sicurezza imposti dalla Direttiva a quei soggetti che vengono definiti fornitori di servizi digitali. Non verrà, pertanto, approfondito il settore relativo ai fornitori di servizi essenziali.

Ciò premesso, i fornitori di servizi digitali comprendono qualsiasi persona giuridica che fornisce un servizio digitale e più specificamente un marketplace, un motore di ricerca o, per quanto di interesse in questa sede, un servizio di cloud computing. La loro regolamentazione, per quanto riguarda i requisiti di sicurezza e gli obblighi di notifica, è giustificata dal fatto che un numero sempre crescente di aziende dipende, al giorno d'oggi, da questi soggetti per la fornitura dei propri servizi. Di conseguenza, una interruzione del servizio digitale potrebbe avere un impatto sulle principali attività economiche e sociali dell'Unione[42]. Va notato che,

[42] Cfr. a tal riguardo il considerando 48 della Direttiva NIS, che recita come segue: "*la sicurezza, la continuità e l'affidabilità del tipo di servizi digitali di cui alla presente direttiva sono essenziali per il buon funzionamento di molte imprese. Un'interruzione di tale servizio digitale potrebbe impedire la fornitura di altri servizi che si basano su di esso e potrebbe quindi avere un impatto sulle principali attività economiche e sociali nell'Unione. Tali servizi digitali potrebbero pertanto rivestire un'importanza cruciale per il buon funzionamento delle imprese che dipendono da esse e, inoltre, per la partecipazione di tali imprese al mercato interno e agli scambi transfrontalieri in tutta l'Unione. Quei fornitori di servizi digitali soggetti alla presente direttiva sono quelli che si ritiene offrano servizi digitali sui quali molte imprese dell'Unione fanno sempre più affidamento*".

rispetto agli operatori dei servizi essenziali, la Direttiva NIS non impone agli Stati membri di identificare specificamente e nel dettaglio i destinatari della norma, garantendo in questo modo un approccio globale.

Per quanto di interesse, un **servizio di cloud computing è considerato un servizio digitale che consente l'accesso a un pool scalabile ed elastico di risorse informatiche condivise.**[43]

La Direttiva descrive, all'articolo 16, le **misure di sicurezza** che i fornitori di servizi digitali dovrebbero adottare al fine di mitigare i rischi che minacciano la sicurezza della rete e dei sistemi informatici che utilizzano per la fornitura del loro servizio. Lo stesso articolo regola il **processo di notifica degli incidenti**, che i fornitori di servizi digitali dovrebbero seguire per conformarsi alle disposizioni della Direttiva.

L'articolo 16, paragrafo 1, elenca gli elementi che devono essere presi in considerazione da un fornitore di servizi digitali quando identifica ed adotta misure di sicurezza per la sua rete, ovvero:

a) la sicurezza dei sistemi e delle strutture,
b) la gestione degli incidenti,
c) gestione della continuità operativa,
d) attività di monitoraggio, audit e collaudo,
e) conformità con gli standard internazionali.

Come anticipato in premessa, la Commissione, in virtù dell'articolo 16(8) della Direttiva NIS, ha emanato un **regolamento di esecuzione** che specifica ulteriormente questi elementi. La necessità di una misura legislativa aggiuntiva che chiarisca le disposizioni della Direttiva NIS, per quanto riguarda gli obblighi di i fornitori di servizi digitali interessati, è stata considerata essenziale. La ragione di tale scelta sembra da rinvenirsi nel fatto che i fornitori di servizi digitali, contrariamente agli operatori di servizi essenziali, sono liberi di adottare misure tecniche e organizzative che ritengono appropriate e proporzionate per gestire il rischio rappresentato dalla sicurezza dei loro sistemi. A tal fine, gli orientamenti e i chiarimenti forniti dal regolamento di esecuzione contribuiscono affinché i fornitori di servizi digitali nell'Unione adottino, nella massima misura possibile, un approccio comune per affrontare la questione.

In aggiunta ai requisiti di sicurezza sopra dettagliati, per consentire a un fornitore di servizi digitali di salvaguardare la sicurezza della sua rete e del suo sistema di informazione, è stato considerato necessario imporre una procedura di notifica degli incidenti. L'obbligo dei fornitori di servizi digitali di notificare eventuali incidenti che abbiano potenzialmente un impatto sostanziale sulla fornitura del loro servizio è regolato dall'articolo 16 par. 3 e 4.

In tale contesto, gli Stati membri assicurano che i fornitori di servizi digitali **notifichino all'autorità competente o al CSIRT qualsiasi incidente che abbia un impatto sostanziale sulla fornitura del loro servizio**. L'articolo 16, paragrafo 4, menziona i parametri da prendere in considerazione per determinare se l'impatto di un incidente è sostanziale, vale a dire:

a) il numero di utenti interessati dall'incidente, in particolare gli utenti che si affidano al servizio per la fornitura di i propri servizi;
b) la durata dell'incidente;
c) la diffusione geografica per quanto riguarda l'area interessata dall'incidente;

[43] Articolo 4(19) e considerando 17 Direttiva NIS.

d) l'entità dell'interruzione del funzionamento del servizio;
e) l'entità dell'incidente sulle attività economiche e sociali.

Questi parametri sono ulteriormente specificati nel regolamento di esecuzione[44].

La regolamentazione più dettagliata degli obblighi previsti per i fornitori di servizi digitali – rispetto a quelli indicati per i fornitori di servizi essenziali – in termini di requisiti di sicurezza e di notifica è rinvenibile anche nel contestuale obbligo di notificare un incidente solo nei casi in cui hanno accesso alle informazioni necessarie per valutare l'impatto di tale incidente. Inoltre, nel caso di fornitori di servizi digitali, contrariamente agli operatori di servizi essenziali, le autorità competenti prendono provvedimenti, se necessario, mediante misure di vigilanza ex post, se tali misure siano proposte dallo stesso fornitore di servizi digitali o da un utente o da un'altra autorità competente.

L'approccio più chiaro della Direttiva nei confronti dei fornitori di servizi digitali, per quanto riguarda i requisiti di sicurezza e di notifica, nonché la loro supervisione ex post da parte delle autorità competenti, è evidente del resto rinvenibile in tutto il testo normativo. Oltre ai principali articoli della Direttiva, molti dei suoi considerando affrontano ampiamente la questione. Il considerando 49, ad esempio, sottolinea che i fornitori di servizi digitali dovrebbero essere liberi di adottare le misure che ritengono appropriate per gestire i rischi presentati ai loro sistemi. Nello stesso contesto, il considerando 57 riconosce le differenze tra gli operatori di servizi essenziali e fornitori di servizi digitali e suggerisce che gli Stati membri non dovrebbero identificare i fornitori di servizi digitali e allo stesso tempo dovrebbero perseguire un diverso livello di armonizzazione in relazione a questi due gruppi di soggetti interessati dalla normativa.

L'approccio più morbido nei confronti dei fornitori di servizi digitali si basa principalmente sulla diversa natura delle infrastrutture che utilizzano e dei servizi che essi rendono ai cittadini europei. Non è senza significato che il termine "*essenziale*" distingue i servizi forniti dagli operatori di servizi essenziali, ma è anche incluso nella loro definizione. Inoltre, la distinzione "*a favore*" dei fornitori di servizi digitali ha un ulteriore vantaggio, in quanto lascia loro una maggiore libertà di condurre attività commerciale, che è considerato un fattore determinante per il loro successo. Questa è anche la conclusione a cui è giunta l'ENISA (la *European Union Agency for Network and Information Security*[45]), che, nel suo intervento sulla questione relativa all'imposizione di un obbligo di notifica di incidenti informatici, rilasciato nel 2017 per i DSP nel contesto del documento della Direttiva NIS, ha osservato che "*A questo proposito, l'approccio meno invasivo mira ad evitare di sovraccaricare i DSP, senza ostacolare la capacità dell'UE di reagire agli incidenti di cyber security in modo rapido ed efficiente*[46]".

La tendenza ad una regolamentazione meno invasiva dei fornitori di servizi digitali in termini di requisiti di sicurezza e di notifica è evidente anche nel relativo obbligo di notifica di incidenti solo nei casi in cui essi abbiano accesso alle informazioni necessarie per valutarne l'impatto effettivo[47]. Inoltre, nel caso dei fornitori di servizi digitali, contrariamente agli operatori di servizi essenziali, le autorità competenti sono tenute a

[44] Articoli 3 e 4 del regolamento di applicazione.
[45] https://www.ENISA.europa.eu.
[46] https://www.ENISA.europa.eu/publications/incident-notification-for-dsps-in-the-context-of-the-nis-directive.
[47] Articolo 16(4) Direttiva NIS.

prendere provvedimenti, se necessario, mediante misure di vigilanza *ex post,* e solo ove coinvolti dallo stesso fornitore di servizi digitali o da un utente o da un'altra autorità competente[48].

Ad ogni buon conto, si è posto il dubbio che questo trattamento di favore non dovrebbe essere garantito, specificamente nel caso in cui vi siano conseguenze che impattino direttamente sui c.d. servizi essenziali. Ad esempio, potrebbero esservi casi in cui gli operatori di servizi essenziali si affidano ai fornitori di servizi digitali per fornire i propri servizi: si pensi, ad esempio, ad un ospedale (da intendersi quale operatore di servizi essenziali attivo nel settore sanitario) che ospita le cartelle dei propri pazienti nel cloud (e quindi attraverso l'intervento di un fornitore di servizi digitali che eroghi servizi di cloud computing). È stato sollevato, pertanto, il dubbio che tali prestatori di servizi digitali dovrebbero essere trattati in modo diverso. Invero, la Direttiva NIS, ad eccezione di alcuni casi di sicurezza nazionale e di mantenimento dell'ordine pubblico, scoraggia fortemente gli Stati membri dall'imporre ulteriori requisiti di sicurezza e di notifica ai fornitori di servizi digitali. Tuttavia, nel testo vi sono diversi riferimenti che lasciano spazio per una lettura leggermente diversa. Il considerando 54, ad esempio, prevede che "*laddove le amministrazioni pubbliche degli Stati membri utilizzino i servizi offerti da fornitori di servizi digitali, in particolare i servizi di cloud computing, esse potrebbero voler richiedere ai fornitori di tali servizi misure di sicurezza aggiuntive oltre a quelle che i fornitori di servizi digitali normalmente offrirebbero in conformità ai requisiti della presente Direttiva. In questo caso, esse dovrebbero essere poste in grado di farlo attraverso obblighi contrattuali*". Si fa riferimento, a tal riguardo, anche al considerando 56, secondo il quale "*la presente Direttiva non dovrebbe impedire agli Stati membri di adottare misure nazionali che impongano agli enti pubblici di garantire requisiti di sicurezza specifici quando stipulano contratti di servizi di cloud computing. Tali misure nazionali dovrebbero applicarsi all'ente del settore pubblico interessato e non al fornitore di servizi di cloud computing*".

Entrambi i considerando mostrano la stessa preoccupazione, mirata a suggerire come potrebbero essere **rafforzati gli obblighi di sicurezza dei fornitori di servizi digitali** ne caso in cui si verifichino **condizioni speciali**.

Ciò che la Direttiva NIS suggerisce è che, in caso di necessità di ulteriori misure di sicurezza, ciò dovrebbe essere attuato **contrattualmente** tra le parti e non mediante disposizioni di legge. Allo stesso tempo, ogni ulteriore misura di sicurezza nazionale dovrebbe applicarsi agli operatori di servizi essenziali e non ai fornitori di servizi digitali[49]. L'articolo 16 (5) porta alla stessa conclusione definendo che l'onere di notifica di un incidente all'autorità competente, anche nei casi in cui l'operatore di servizi essenziali si affidi a un

---

[48] Cfr. il considerando 60 della Direttiva NIS, che recita: "*I prestatori di servizi digitali dovrebbero essere soggetti ad attività di vigilanza ex post semplificate e reattive, giustificate dalla natura dei loro servizi e delle loro operazioni. L'autorità competente interessata dovrebbe pertanto adottare misure solo quando ottiene la prova, ad esempio dallo stesso fornitore di servizi digitali, da un'altra autorità competente, compresa un'autorità competente di un altro Stato membro, o da un utente del servizio, che un fornitore di servizi digitali non rispetta gli obblighi della presente direttiva, in particolare in seguito al verificarsi di un incidente. Pertanto, l'autorità competente non dovrebbe avere un obbligo generale di vigilanza sui fornitori di servizi digitali*". Cfr. anche l'articolo 17 della Direttiva.

[49] Cfr. a tal riguardo l'Articolo 16(10) della Direttiva NIS: "*Fatto salvo l'articolo 1, paragrafo 6, gli Stati membri non impongono ulteriori requisiti di sicurezza o di notifica ai fornitori di servizi digitali*". L'Articolo 1(6) recita come segue: "*La presente direttiva non pregiudica le azioni intrapreso dagli Stati membri per salvaguardare le loro funzioni statali essenziali, in particolare per salvaguardare la sicurezza nazionale, comprese le azioni a tutela delle informazioni la cui divulgazione è considerata dagli Stati membri contraria agli interessi essenziali della loro sicurezza e per mantenere la legge e l'ordine, in particolare per consentire indagine, accertamento e perseguimento di reati*".

fornitore di servizi digitali di terze parti per la fornitura del servizio, deve rimanere inteso in capo agli operatori di servizi essenziali.

Per quanto attiene il sistema sanzionatorio, infine, la Direttiva NIS lascia agli Stati membri un margine di discrezionalità riguardo al tipo e alla natura delle sanzioni applicabili, a condizione che siano effettive, proporzionate e dissuasive. Nell'esercitare tale discrezionalità, il governo italiano ha ritenuto di stabilire che le autorità competenti potranno applicare **sanzioni amministrative** fino a 150.000 euro in caso di violazione da parte degli operatori di servizi essenziali (e dei fornitori di servizi digitali) degli obblighi previsti dal decreto. Si tratta di un approccio in linea con quello seguito da altri Stati membri. Infatti, mentre la Germania ha previsto sanzioni fino a 100.000 euro per le violazioni della propria normativa di recepimento della Direttiva, in altri casi, come ad esempio in Repubblica Ceca, le sanzioni salgono fino a circa 200.000 euro.

I principi e le misure di sicurezza applicabili ai Cloud Service Providers: l'approccio della PSD2

Il 13 gennaio 2016 è entrata in vigore la direttiva 2015/2366/(UE) sui servizi di pagamento prestati nel mercato interno europeo (PSD2) che abroga la precedente direttiva 2007/64/CE (PSD) e introduce significative novità nel mondo dei pagamenti in termini di ruoli e responsabilità, attori coinvolti e soluzioni tecnologiche a supporto. Gli Stati membri hanno avuto due anni di tempo per recepire la direttiva all'interno della propria legislazione nazionale e il Governo italiano l'ha resa operativa il 13 gennaio 2018 con la pubblicazione sulla Gazzetta Ufficiale del d.lgs n. 218/2017.
La PSD2 ha, tra l'altro, introdotto tre importanti nuovi player del settore:

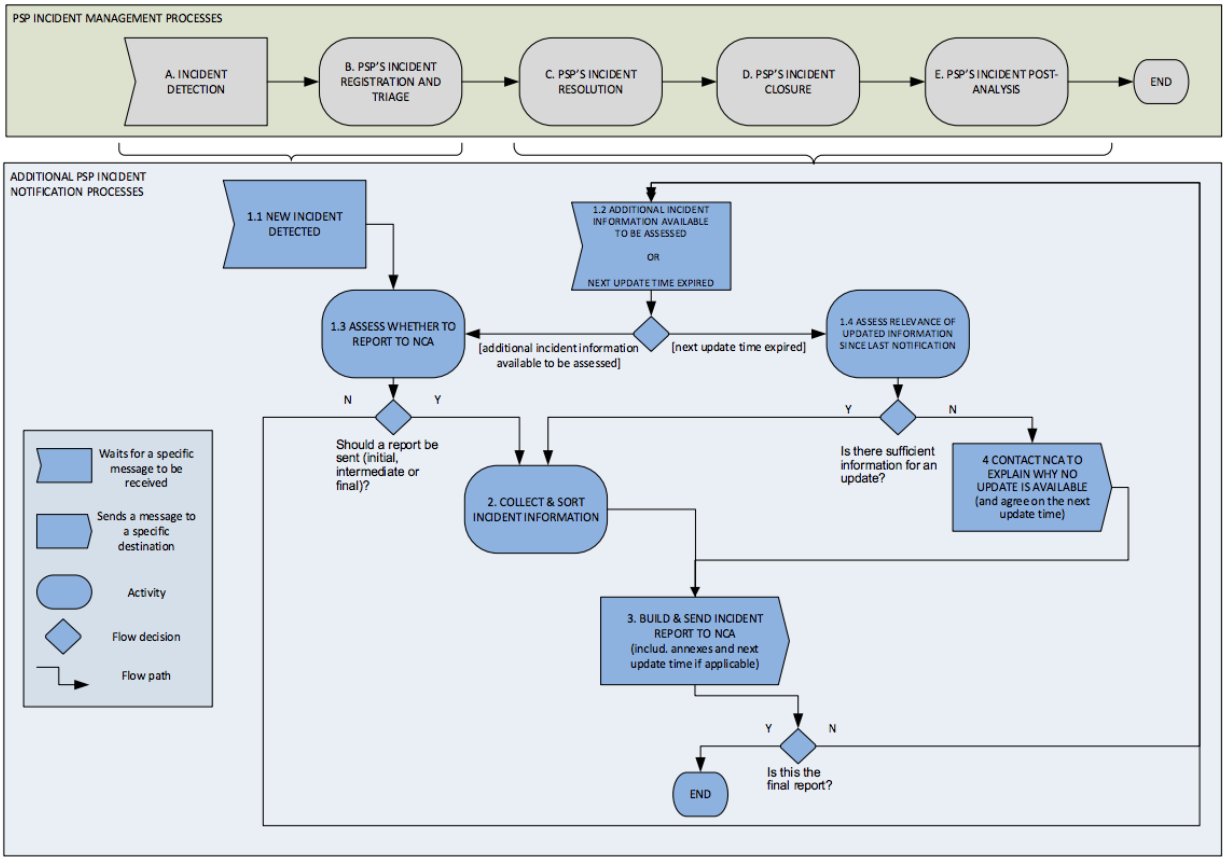
1) gli **AISP** (Account Information Service Provider), fornitori di servizi con accesso alle informazioni sul conto dei clienti delle banche in grado di analizzare il comportamento di spesa di un utente o aggregare i dati da diverse banche in un'unica piattaforma;
2) i **PISP** (Payment Initiation Service Provider), fornitori di servizi di pagamento che, a tutti gli effetti, possono svolgere molte delle attività svolte tipicamente da banche e istituti di pagamento;
3) i **CISP** (Card Issuing Service Provider), prestatori di servizi di pagamento basati su carta che permettono di sapere se sul conto del pagatore vi è disponibilità dell'importo richiesto perché la transazione vada a buon fine. Il CISP non vede quanti soldi ci sono sul conto dell'utente, ma fornisce solo risposta positiva o negativa al momento dell'operazione di pagamento.

I requisiti per la "licenza" al fine di operare quale PISP, AISP, CISP (qui cumulativamente definiti "**PSP**" o "**Payment Service Provider**") sono fissati sia dalla PSD2 che dalle guidelines fornite dall'EBA e dai regolamenti e disposizioni attuative fornite a livello nazionale, con particolare riferimento al quadro regolamentare di Banca d'Italia, anche nel rispetto del Testo Unico Bancario - D. Lgs. 1 settembre 1993, n. 385 (TUB).
Analizzando la documentazione necessaria da presentare a Banca d'Italia, è interessante notare, in alcuni passaggi, la stretta correlazione con la documentazione richiesta per l'"**allineamento" al GDPR** ed è quindi importante, ad avviso di chi scrive, coordinare le due attività (quella di allineamento alla PSD2 e quella di allineamento al GDPR) in modo da evitare overlapping documentali che possano determinare contraddizioni in termini di operatività, con particolare riferimento alle procedure da attivare in caso di data breach e/o incidente informatico.
Tra la documentazione di rilievo, applicabile ai PSP, si segnala la seguente:

a) una descrizione dei dispositivi di governo societario dei **meccanismi di controllo interno**, ivi comprese le procedure amministrative, di gestione del rischio e contabili, del richiedente, che dimostri che tali dispositivi di governo societario, meccanismi di controllo e procedure siano proporzionati, appropriati, validi ed adeguati;
b) una descrizione della **procedura** esistente per **monitorare e gestire gli incidenti** relativi alla sicurezza e i reclami dei clienti in materia di sicurezza e per darvi seguito, compreso un meccanismo di notifica degli incidenti che tenga conto degli obblighi di notifica dell'istituto di pagamento di cui all'articolo 96 PSD2;
c) una descrizione della **procedura** esistente per **archiviare, monitorare, tracciare e limitare l'accesso** in ordine ai dati sensibili relativi ai pagamenti;

d) una descrizione delle disposizioni in materia di **continuità operativa**, tra cui l'individuazione chiara delle operazioni critiche, piani di emergenza efficaci e una procedura per testare periodicamente tali piani e riesaminarne l'adeguatezza e l'efficacia.

Fermo quanto sopra, la Banca d'Italia (e le altre banche nazionali europee di riferimento) autorizza i PSP a condizione che abbiano stipulato una polizza di assicurazione della responsabilità civile o analoga forma di garanzia per i danni arrecati nell'esercizio dell'attività derivanti da condotte proprie o di terzi. Le società di assicurazione si stanno attrezzando al fine di fornire prodotti assicurativi idonei a quanto richiesto dalle Banche Centrali, al fine di assicurare i rischi connessi ai cosiddetti incidenti di sicurezza informatici.
Soffermandoci, in particolare, sugli incidenti informatici, è doveroso richiamare le **guidelines dell'EBA** come da standard pubblicato quale Annex 1 del Final Report EBA del 27 luglio 2017, n. EBA/GL/2017/[50]. Le Guidelines, di 83 pagine, forniscono un dettagliato quadro su come le società, che intendono svolgere attività quale PSP, debbano gestire i cosiddetti "incidenti informatici", definendo non solo un flusso di attività conseguenti ad un incidente ma anche le procedure di notifica e i modelli di reportistica.
Nel diagramma qui di seguito, viene rappresentato il processo di notifica da parte di un PSP alla autorità bancaria centrale nazionale (in Italia Banca d'Italia), relativo ad un incidente informatico.



Fonte: https://eba.europa.eu

[50] https://eba.europa.eu/documents/10180/1914076/Guidelines+on+incident+reporting+under+PSD2+%28EBA-GL-2017-10%29.pdf

La **procedura per monitorare e gestire gli incidenti** relativi alla sicurezza è **sensibilmente analoga** alla **procedura necessaria per individuare un *data breach*** relativo a dati personali ai sensi del GDPR. Potrebbe quindi essere estremamente importante valutare l'**opportunità**, per i PSP, l'**accorpamento della documentazione** relativa a tale procedura sia per **economia documentale** che per **ottimizzare le attività** in caso di incidente informatico relativo a dati bancari, che comporti anche un indebito accesso (o peggio diffusione) di dati personali.

Secondo quanto previsto dall'art. 36 della PSD2, gli Stati membri provvedono affinché gli istituti di pagamento abbiano accesso ai servizi relativi ai conti di pagamento degli enti creditizi in maniera obiettiva, proporzionata e non discriminatoria. L'accesso è sufficientemente ampio da consentire all'istituto di pagamento di fornire servizi di pagamento in modo agevole ed efficiente. L'ente creditizio fornisce all'autorità competente motivazioni debitamente circostanziate per eventuali rifiuti.

In buona sostanza, quanto previsto all'art. 36 della PSD2, impone quello che impropriamente è stato definito "open banking", da intendersi quale apertura del mercato di una serie rilevante di servizi finanziari a soggetti terzi (i PSP) che, grazie anche alla tecnologia di riferimento adottata, potranno garantire servizi più efficienti, meno costosi e trasparenti.

Il libero accesso alle Application Program Interface (API) decorre dal 14 settembre 2019, salvo dilazioni concesse dalle singole Banche Centrali dei paesi membri, caso per caso. È evidente quindi che, da tale data, tutti gli istituti bancari e di pagamento sono tenuti ad adottare nuovi standard di sicurezza proprio per garantire maggiore affidabilità del servizio bancario e per far ciò potranno avvalersi anche di soggetti terzi specializzati.

D'altra parte, i PSP, per poter operare devono superare attente valutazioni da parte delle Banche Centrali di riferimento che analizzino in dettaglio le procedure adottate dalle aziende in caso di incidente informatico, e la coerenza e consistenza degli **investimenti** che la società intende effettuare in **ambito sicurezza informatica**. Questi investimenti devono essere congrui con le prospettive di crescita della società secondo il piano triennale che deve essere consegnato alla Banca Centrale di riferimento (in Italia Banca d'Italia) in sede di autorizzazione ad operare quale PSP e dovrà avere una sua logica sostenibile. Inoltre, le Banche centrali avranno il delicato compito di monitorare costantemente i PSP autorizzati, al fine di verificare che quanto dichiarato in sede di autorizzazione sia correttamente implementato.

L'aumento e la diversificazione delle minacce registrate, specie nel campo dei pagamenti elettronici e attraverso internet, richiede che gli intermediari accrescano, oltre alle misure di protezione, anche la capacità di individuare e gestire prontamente eventuali incidenti e attacchi cyber.

Al fine di mitigare il rischio di frodi, anche nella prospettiva di accrescere l'accettazione e diffusione di strumenti di pagamento innovativi, la Direttiva PSD2 prevede una maggiore attenzione alla protezione dei dati sensibili relativi ai pagamenti, incluse le credenziali di autenticazione. I PSP dovranno, pertanto, avere strutturato un processo per l'archiviazione, il monitoraggio, la tracciabilità e la limitazione dell'accesso ai dati sensibili relativi ai pagamenti, che includa in particolare:

a) la definizione di una policy sul diritto di accesso, che disciplini l'accesso a tutti i componenti e i sistemi dell'infrastruttura informatica utilizzati per il trattamento di tali dati, inclusi i database e i sistemi di back up;
b) l'identificazione dei soggetti che hanno accesso ai dati sensibili relativi ai pagamenti.

Da quanto sopra, traspare il collegamento tra la normativa di cui alla PSD2 e quella di cui al GDPR e la maggiore tutela degli utenti in relazione ai dati personali e, a tal fine, si rinvia a quanto previsto al successivo punto 5 sotto.

Le differenze e le sovrapposizioni tra gli obblighi previsti dal GDPR, dalla NIS e dalla PSD2

Sia il GDPR che la Direttiva NIS, nonché la PSD2, hanno un impatto rilevante sui servizi di cloud computing. I fornitori di servizi cloud che trattano dati personali rientrano infatti all'interno della categoria di "titolari" (qualora determinino le finalità e i mezzi del trattamento sulla base di una idonea informativa fornita all'interessato) o, con maggiore frequenza, in quella di "responsabili" del trattamento di dati personali (qualora trattino i dati per conto del titolare) e sono pertanto tenuti al rispetto dei principi predisposti dal GDPR, compresi quelli in materia di sicurezza. Il quadro si complica se si considera che le persone giuridiche che forniscono servizi cloud sono considerati fornitori di servizi digitali (come certamente accade nel caso dei fornitori di servizi di informazione sui conti ex PSD2 in favore di istituti di pagamento) e sono pertanto destinatari degli obblighi di sicurezza e di notifica previsti dalla Direttiva NIS.

Da questa "**doppia qualificazione**" dei fornitori di servizi cloud come **titolari/responsabili** del trattamento ai sensi del GDPR e come **fornitori di servizi digitali** ai sensi della Direttiva NIS, inclusi eventuali **fornitori di servizi di pagamento** (PISP) o di informazione su conti correnti bancari (AISP) ex PSD2, deriva inevitabilmente a carico di tali soggetti una sovrapposizione tra gli obblighi prescritti dalle normative in esame in materia di sicurezza e di notifica di eventuali incidenti informatici.

È pertanto evidente che, nella pratica, gli obblighi previsti dal Regolamento e dalla Direttiva NIS ma, come abbiamo visto, anche quelli posti dalla PSD2 possono **parzialmente sovrapporsi**, pur mantenendo oggetti di tutela e quindi ambiti applicativi differenti. Se, da un lato, questa parziale sovrapposizione può ingenerare confusione specialmente nella gestione di obblighi simili ma con presupposti diversi o da adempiersi con modalità differenti, dall'altro, il fatto che il GDPR, la Direttiva NIS e la PSD2 impongano alle aziende sforzi applicativi in parte simili è da considerarsi virtuoso poiché consente alle aziende di **ottimizzare**, invece che moltiplicare, le risorse investite ai fini della compliance con i diversi requisiti normativi. Al contempo, un'adeguata comprensione (oltre che dei punti di contatto) delle differenze tra le prescrizioni contenute nelle normative in esame risulta di importanza essenziale proprio ai fini di una corretta gestione ed applicazione degli obblighi in materia di sicurezza previsti rispettivamente da GDPR, NIS e PSD2. Il presente paragrafo mira pertanto a mettere in evidenza le sovrapposizioni, oltre che le differenze, tra gli obblighi previsti dai tre testi normativi.

3.1 Le sovrapposizioni tra NIS e GDPR

Come visto al punto 3, i fornitori di servizi cloud rientrano all'interno della definizione di fornitori di servizi digitali della Direttiva NIS e sono pertanto tenuti al rispetto delle disposizioni della Direttiva. Al contempo, ogniqualvolta i fornitori di servizi cloud trattino dati personali, questi assumono la qualifica, a seconda dei casi, di titolari o responsabili del trattamento. I fornitori di servizi cloud devono quindi spesso prendere in considerazione gli obblighi imposti da entrambe le normative.

Prima di esaminare le possibili sovrapposizioni tra gli obblighi imposti dalla Direttiva e dal Regolamento, è opportuno sottolineare le importanti differenze tra i due testi normativi. Mentre infatti la Direttiva NIS mira a conseguire un livello comune ed elevato di sicurezza della rete e dei sistemi informativi nell'Unione, il Regolamento stabilisce "norme relative alla protezione delle persone fisiche con riguardo al trattamento dei

dati personali, nonché norme relative alla libera circolazione di tali dati". In altre parole, mentre la Direttiva NIS ha come obiettivo specifico il rafforzamento della sicurezza informatica entro in confini dell'Unione Europea, il GDPR mira a proteggere il diritto alla protezione dei dati personali quale diritto fondamentale delle persone fisiche sancito all'articolo 8 della Carta dei Diritti Fondamentali dell'Unione Europea e all'articolo 16(1) del Trattato sul Funzionamento dell'Unione Europea, assicurando al contempo la libera circolazione dei dati all'interno dei confini dell'Unione.

La Direttiva NIS dà evidenza della demarcazione tra il proprio campo di applicazione, definito all'articolo 1, e quello della normativa europea sulla protezione dei dati personali a cui viene fatto un rimando all'articolo 2. L'Articolo 2 della Direttiva infatti chiarisce che il trattamento dei dati personali ai sensi della Direttiva NIS è effettuato nel rispetto della normativa europea in materia di protezione dei dati personali. Gli obblighi previsti dal GDPR andranno pertanto a sommarsi a quelli previsti dalla Direttiva NIS ogniqualvolta le reti e sistemi informativi siano utilizzati per trattare (anche) dati personali.

Nonostante la diversità tra gli ambiti di applicazione delle due normative e quindi anche tra i rischi che le due normative mirano a mitigare (i.e., rischi a cui sono esposti le reti e i sistemi informativi e i dati a questi associati v. rischi a cui sono esposti i dati personali e quindi gli individui), le disposizioni in materia di sicurezza da queste previste presentano vari punti di sovrapposizione.

In primo luogo, sia la Direttiva NIS che il GDPR impongono l'implementazione di misure "**adeguate**" al livello di rischio[51] mentre la Direttiva NIS, a differenza del GDPR, richiede anche che tali misure siano "proporzionate alla gestione dei rischi".[52] Inoltre, entrambi i testi normativi includono i tre elementi fondamentali della sicurezza informatica, ovvero confidenzialità, integrità e disponibilità, conosciuti con l'acronimo "**CIA**" (Confidentiality, Integrity, Availability).[53]

Occorre, inoltre, sottolineare come il GDPR ponga l'accento non solo sull'adempimento degli obblighi imposti dal Regolamento ma anche sulla **capacità di dimostrare** che il trattamento dei dati personali è effettuato nel rispetto del Regolamento.[54] Sebbene il principio della responsabilizzazione non emerga in modo esplicito dal testo della Direttiva NIS, il Regolamento di esecuzione 2018/151 impone ai fornitori di servizi digitali di "rendere disponibile la documentazione adeguata per consentire all'autorità competente di verificare la conformità con gli elementi di sicurezza".[55] L'obbligo per i fornitori di servizi digitali di documentare in modo adeguato le misure adottate e di rendere tale documentazione disponibile in caso di richiesta da parte dell'autorità competente sembra coerente con il principio di accountability del GDPR.

Inoltre, la Direttiva NIS dispone che le misure di sicurezza che devono essere implementate al fine di gestire il rischio tengano conto, *inter alia*, della conformità con le norme internazionali.[56] Questa disposizione ricorda l'articolo 32 GDPR nella parte in cui prevede che l'adesione a un codice di condotta o a un

---

[51] Articolo 32(1) GDPR, Articolo 16(1) Direttiva NIS.
[52] Articolo 16(1) Direttiva NIS.
[53] https://ico.org.uk/for-organisations/the-guide-to-nis/gdpr-and-nis/

[54] Articolo 5(2) GDPR e Articolo 24(1) GDPR.
[55] Articolo 2(6) Regolamento di esecuzione 2018/151. Hon, W. Kuan, Cloud Service Providers Under the NIS Directive – The UK's Implementation (With GDPR Comparisons), June 13, 2018, p.5, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3200149.

[56] Articolo 16(1)(e) Direttiva NIS.

meccanismo di certificazione possa essere utilizzata come elemento per dimostrare la conformità ai principi di sicurezza imposti dal Regolamento.[57]

Complessivamente, gli obblighi in materia di sicurezza imposti ai CSP (in qualità di titolari o responsabili ai sensi del GDPR e in qualità di fornitori di servizi digitali ai sensi della Direttiva NIS) sono definiti in modo **più specifico e dettagliato dalla Direttiva NIS** e dal relativo Regolamento di esecuzione rispetto al GDPR. In caso di incertezza su quali misure di sicurezza debbano essere applicate per garantire un'adeguata tutela ai dati personali, i CSPs potrebbero pertanto utilizzare i parametri dettati dalla Direttiva NIS come guida per orientare le proprie scelte in termini di sicurezza anche rispetto al GDPR.[58]

Un altro importante ed evidente punto di sovrapposizione tra le disposizioni del GDPR e quelle della Direttiva NIS va individuato negli **obblighi di notifica** di un incidente informatico ai sensi dell'articolo 16 della Direttiva NIS e negli obblighi di notifica di un *data breach* ai sensi dell'articolo 33 del GDPR. La Direttiva NIS infatti impone ai fornitori di servizi digitali di notificare all'autorità competente o al CSIRT qualsiasi incidente che abbia un impatto rilevante sulla fornitura del loro servizio. Qualora poi l'incidente in questione abbia compromesso anche dati personali, il fornitore di servizi cloud sarà tenuto anche al rispetto dell'articolo 33 GDPR e dovrà quindi procedere alla notifica della violazione all'autorità di controllo competente o a informare il titolare senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione nei casi in cui il CSP tratti i dati in qualità di responsabile del trattamento.

In alcuni casi, un incidente potrà rappresentare contestualmente un incidente informatico ai sensi della NIS e un *data breach* ai sensi del GDPR, come nel caso in cui i dati digitali compromessi dall'incidente in questione includano anche dati personali. In altri casi, l'incidente informatico ai sensi della NIS può *portare* a una violazione dei dati personali come nel caso di un CSP che abbia subito una iniziale intrusione nel proprio sistema informatico e che riscontri, proprio a causa di questa iniziale intrusione, anche una violazione dei dati personali di cui è in possesso.[59]

La stessa Direttiva NIS dà atto delle possibili sovrapposizioni tra incidente informatico e *data breach*. Il considerando 63 infatti riconosce che "[i]n molti casi gli incidenti compromettono dati personali. Al riguardo è opportuno che le autorità competenti e le autorità responsabili della protezione dei dati collaborino e si scambino informazioni su tutti gli aspetti pertinenti per affrontare le violazioni ai dati personali determinate dagli incidenti".[60]

Alcune importanti differenze tra le procedure di notifica in caso di incidente informatico ai sensi della Direttiva NIS da un lato e di *data breach* ai sensi del GDPR dall'altro tuttavia permangono rispetto (a) ai presupposti per procedere alla notifica, (2) ai destinatari della notifica, e (3) ai tempi previsti per procedere alla notifica.

Per quanto concerne i presupposti della notifica, l'articolo 16 della Direttiva NIS prevede che i fornitori di servizi essenziali siano tenuti alla notifica solo nei casi in cui l'incidente abbia avuto un **impatto rilevante sulla fornitura del suo servizio**. Lo stesso articolo individua i parametri di cui tenere conto al fine di

[57] Hon, W. Kuan, Cloud Service Providers Under the NIS Directive – The UK's Implementation (With GDPR Comparisons), June 13, 2018, p.6.
[58] Ibid.
[59] https://ico.org.uk/for-organisations/the-guide-to-nis/gdpr-and-nis/
[60] Considerando 63 Direttiva NIS.

determinare se l'impatto di un incidente sia stato o meno sostanziale (ad es., il numero degli utenti interessati, la durata dell'incidente, la diffusione geografica relativamente all'area interessata dall'incidente), parametri che sono stati ulteriormente elaborati nel Regolamento di esecuzione 2018/151. Ai sensi del GDPR, invece, l'elemento determinante per valutare se una violazione vada o meno notificata va individuata nella possibilità che tale violazione abbia **effetti avversi significativi sugli individui**. L'articolo 33 GDPR infatti dispone che il titolare dovrà procedere alla notificazione della violazione "a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche".

Per quanto riguarda i **destinatari della notifica**, mentre la violazione dei dati personali deve essere notificata all'Autorità Garante della Protezione dei dati personali (in Italia, il Garante Privacy), gli incidenti informatici ai sensi della NIS devono essere notificati alle autorità NIS competenti o al CSIRT. Lo stesso incidente informatico può quindi essere oggetto di due separate notifiche a due distinte autorità. Inoltre, mentre il GDPR dispone all'articolo 34 GDPR che anche gli interessati debbano essere resi edotti della violazione quando questa sia suscettibile di rappresentare un rischio elevato per i diritti e le libertà delle persone fisiche, la Direttiva NIS non prevede un analogo obbligo di comunicazione agli individui coinvolti. L'articolo 16(7) della Direttiva prevede piuttosto la possibilità per l'autorità competente o per il CSIRT di "informare il pubblico riguardo ai singoli incidenti o chiedere al fornitore di servizi digitali di provvedervi, qualora sia necessaria la sensibilizzazione del pubblico per evitare un incidente o gestirne uno in corso, o qualora la divulgazione dell'incidente sia altrimenti nell'interesse pubblico".

Per quanto riguarda i **tempi per la notifica**, a differenza dell'articolo 33 GDPR che impone al titolare di notificare un eventuale *data breach* entro 72 ore dal momento in cui ne è venuto a conoscenza (e a motivare eventuali ritardi), l'Articolo 16 della Direttiva non quantifica in termini di ore/giorni il termine per la notifica ma dispone, con una formulazione generica, che i fornitori di servizi digitali notifichino l'autorità competente "senza indebito ritardo". La normativa nazionale di attuazione della Direttiva può tuttavia prevedere dei termini precisi per procedere alla notifica. Ad esempio, la normativa di attuazione del Regno Unito ha allineato i termini per la notifica di incidenti informatici ai sensi della Direttiva NIS ai tempi per la notifica dei *data breach*. Gli incidenti informatici devono infatti essere notificati in ogni caso non oltre 72 ore da quando il fornitore di servizi digitali ne è venuto a conoscenza.[61] Il decreto italiano di attuazione della Direttiva ha invece mantenuto una formulazione generica disponendo che i fornitori di servizi digitali debbano notificare "al CSIRT italiano e, per conoscenza, all'autorità competente NIS, *senza ingiustificato ritardo*, gli incidenti aventi un impatto rilevante sulla fornitura" del loro servizio.[62]

Alla luce di quanto sopra, in alcuni casi, il CSP che abbia subito un incidente rilevante ai sensi sia della Direttiva NIS che del GDPR potrà procedere *contestualmente* alla notifica ai sensi delle due normative. In altri casi, il CSP potrebbe rendersi conto solo dopo un variabile lasso di tempo che l'incidente informatico già

---

[61] Articolo 12(6)(a), SI 2018/506, https://www.legislation.gov.uk/uksi/2018/506/made. Una importante differenza tuttavia permane tra i termini per la notifica di un *data breach* e i termini per la notifica di un incidente NIS. Infatti, mentre ai sensi dell'articolo 33(1) GDPR le violazioni dei dati personali devono essere notificate all'autorità competente "senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui [il titolare] ne è venuto a conoscenza", lasciando così spazio a una eventuale notifica tardiva purché motivata, il regolamento che ha dato attuazione nel Regno Unito alla Direttiva NIS prevede il termine di 72 come termine ultimo non prorogabile. Hon, W. Kuan, Cloud Service Providers Under the NIS Directive – The UK's Implementation (With GDPR Comparisons), June 13, 2018, p.9.

[62] Articolo 14(4) Decreto Legislativo 18 maggio 2018, n. 65 (enfasi aggiunta).

notificato ai sensi della Direttiva NIS ha compromesso anche dati personali. In questi casi, il CSP procederà alla "seconda" notifica, ovvero quella ai sensi del GDPR, entro 72 ore dal momento in cui è venuto a conoscenza del *data breach*.

La seguente tabella sintetizza le principali differenze tra la procedura di notifica prevista dalla Direttiva NIS e la procedura prevista dal GDPR:

	Direttiva NIS	GDPR
Oggetto della notifica	Incidente: "ogni evento con un reale effetto pregiudizievole per la sicurezza della rete e dei sistemi informativi" (Art. 4 n.7 Direttiva NIS)	Violazione dei dati personali: "la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati" (Ar.4 n.12 GDPR)
Destinatario della notifica	Autorità NIS competente o CSIRT	Garante Privacy del paese ove opera il titolare del trattamento interessato dal Personal Data Breach
Termine	Senza indebito ritardo	Senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui il titolare ne è venuto a conoscenza.
Fonte normativa	Art. 16 comma 3 Direttiva NIS	Art. 33 comma 1 GDPR

3.2 Le sovrapposizioni tra PSD2 e GDPR

Dall'analisi del complesso di norme "comunitarie" e "regolamentari" relative alla PSD2, solo una volta viene fatta menzione del GDPR, e in particolare al punto 4.3 delle Linee Guida EBA/GL/2017/17 in tema di Misure di Sicurezza.

Il punto 4.3 stabilisce, infatti che i prestatori di servizi di pagamento dovrebbero garantire la riservatezza, l'integrità e la disponibilità delle loro risorse logiche e fisiche critiche, e dei dati sensibili per i servizi di pagamento relativi ai loro utenti, sia che essi siano inutilizzati, in transito o in uso. Il punto prosegue, poi, precisando che ***"[s]e i dati comprendono dati personali, tali misure dovrebbero essere attuate conformemente al regolamento (UE) 2016/679 o, se applicabile, al regolamento (CE) n. 45/2001***".

Tra i vari punti di sovrapposizione, che potrebbero determinare una incertezza interpretativa e problematiche gestionali all'interno delle aziende che subiscono un incidente informatico qualificabile sia come incidente di sicurezza ai sensi della PSD2 e delle relative linee guide EBA, sia quale *data breach* ai sensi del GDPR, possono elencarsi le seguenti:

a) inquadramento del PSP quale titolare, responsabile o co-titolare;
b) definizione di dato sensibile ai sensi della PSD2;
c) attivazione delle procedure di sicurezza nelle ipotesi di incidente di sicurezza ai sensi delle citate linee guida EBA;

d) gestione di una unica valutazione di impatto sui rischi al fine di coordinare le previsioni di cui alle citate linee guida EBA e le previsioni del GDPR in materia di DPIA.

a) L'inquadramento del PSP quale titolare, responsabile o co-titolare

Come noto l'art. 4(7) del GDPR definisce "titolare del trattamento" la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali. L'art. 4.8, definisce invece il "responsabile del Trattamento" la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento. Inoltre, l'art. 28, primo comma del GDPR, prevede che qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti GDPR e garantisca la tutela dei diritti dell'interessato.

Orbene, l'art. 66 della PSD2, in tema di disposizioni per l'accesso ai conti di pagamento in caso di servizi di disposizione di ordine di pagamento, stabilisce, al primo comma, quanto segue: "*Gli Stati membri provvedono affinché un pagatore abbia il diritto di avvalersi di un prestatore di servizi di disposizione di ordine di pagamento per ottenere servizi di pagamento a norma del punto 7 dell'allegato I [PSD2]. Il diritto di avvalersi di un prestatore di servizi di disposizione di ordine di pagamento non si applica qualora il conto di pagamento non sia accessibile online*".

Il successivo comma 5, stabilisce poi che: "*La prestazione di servizi di disposizione di ordine di pagamento* ***non è subordinata all'esistenza di un rapporto contrattuale*** *a tale scopo tra i prestatori di servizi di disposizione di ordine di pagamento e i prestatori di servizi di pagamento di radicamento del conto*".

La sostanza di cui all'art. 66, viene poi replicata nel successivo art. 67 della PSD2, in tema di disposizioni per l'accesso alle informazioni sui conti di pagamento e all'utilizzo delle stesse in caso di servizi di informazione sui conti (servizio svolto tipicamente dagli AISP).

Dalla lettura dei commi 1 e 5 degli artt. 66 e 67 della PSD2, si evince che la Banca non può imporre al PSP la stipula di uno specifico contratto per consentire l'accesso alle API della banca al fine di consentire al PSP l'accesso ai dati relativi ai conti di pagamento nel rispetto della PSD2. Questo potrebbe ingenerare il dubbio in relazione all'eventuale stipula tra Banca e PSP del contratto ex art. 28 GDPR sopra citato. Orbene, il PSP, al fine di poter fornire i servizi al cliente finale, dovrà ottenere preventivamente il suo consenso. Sarà quindi l'utente a relazionarsi direttamente con il PSP e dargli apposito consenso espresso.

In considerazione di quanto sopra, e alla luce delle finalità della PSD2 che punta ad una disintermediazione del servizio di pagamento con una sostanziale sostituzione dei PSP a molte delle attività poste oggi in essere da banche e istituti di pagamento, parrebbe, ad avviso di chi scrive, che la posizione del PSP rispetto alla banca o istituto di pagamento con cui si interfaccia per il tramite delle API rese accessibili ai sensi dell'art. 36 della PSD2, rientrerebbe nella fattispecie di cui al citato art. 4(7) GDPR e non già nella fattispecie di cui al successivo art. 4(8.)

Il PSP agisce solo sulla base della specifica autorizzazione del cliente il quale, come detto, si interfaccerà direttamente al PSP accettando le sue condizioni generali del servizio di pagamento offerto e, naturalmente della sua privacy policy.

Diverso sarebbe il discorso nel caso in cui un PSP decida di offrire i suoi servizi tecnologici per la gestione di pagamenti o analisi conti, non già direttamente ai suoi clienti ma alle banche o istituti di pagamento, le quali banche poi utilizzeranno tali servizi per migliore l'offerta ai loro clienti finali. In tal caso, troverà certamente

applicazione la fattispecie di cui all'art. 4(8) GDPR per il PSP e la conseguente necessità del contratto ex art. 28 GDPR. Ma, attenzione, in tali casi il PSP opera come naturale fornitore della banca o istituto di pagamento, e non già quale operatore qualificato ai sensi della PSD2.

D'altra parte, in modo saggio, il legislatore europeo ha specificato, in relazione alla insussistenza di rapporti contrattuali tra banche/istituti di pagamento e PSP, sia all'art. 66 che all'art. 67 PSD2, l'inciso "*a tale scopo*", proprio al fine di chiarire che eventuali ulteriori scopi, tra cui potrebbe rientrare benissimo il contratto ex art. 28 GDPR, sono sostanzialmente ammissibili a seconda dei casi.

Venendo invece alla ipotesi di contitolarità nel trattamento del dato personale, pare opportuno richiamare quanto previsto in materia dall'art. 26 GDPR. Esso prevede, al primo comma quanto segue: "*Allorché due o più titolari del trattamento* ***determinano congiuntamente le finalità e i mezzi del trattamento****, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati*."

In realtà, ad avviso di chi scrive, PSP e banche/istituti di pagamento, difficilmente si troveranno nella condizione di cui all'art. 26 GDPR sopra citato poiché sarà alquanto improbabile che questi player, che operano su livelli sostanzialmente diversi, anche se per molti aspetti omogenei, determinino congiuntamente finalità e mezzi del trattamento dei dati personali.

Tuttavia, tale aspetto, andrà analizzato con estrema cautela e caso per caso, anche in considerazione della mancanza di un coordinamento normativo tra le due norme comunitarie concepite e pubblicate in tempi diversi.

Ove, quindi, in ultima analisi, fosse necessario stipulare tra banche/istituti di pagamento da una parte e PSP dall'altra, un contratto ex art. 26 GDPR, ciò sarà comunque fattibile in considerazione del fatto che il vincolo all'assenza di contrattualistica tra i due soggetti è riferito, come sopra detto, allo specifico scopo della PSD2, in relazione alle modalità di accesso alle API.

b) Definizione di dato sensibile ai sensi della PSD2. Criticità

Come detto in introduzione al paragrafo, dall'analisi del complesso di norme "comunitarie" e "regolamentari" relative alla PSD2, solo una volta viene fatta menzione del GDPR. Dobbiamo andare al punto 4.3 delle Linee Guida EBA/GL/2017/17 in tema di Misure di Protezione, dove troviamo il seguente inciso:

"*I prestatori di servizi di pagamento dovrebbero garantire la riservatezza, l'integrità e la disponibilità delle loro risorse logiche e fisiche critiche, e dei* ***dati sensibili*** *per i servizi di pagamento relativi ai loro utenti, sia che essi siano inutilizzati, in transito o in uso. Se i dati comprendono dati personali, tali misure dovrebbero essere attuate conformemente al regolamento (UE) 2016/679 o, se applicabile, al regolamento (CE) n. 45/2001*".

Preliminarmente si evidenzia come la definizione di "dati sensibili" dal punto di vista strettamente normativo, sia obiettivamente obsoleta (si pensi che la definizione di dato sensibile è rinvenibile nel GDPR solo una volta, in via incidentale e in virgolettato, al considerando n. 10). Infatti i cosiddetti *dati sensibili* possono essere ora considerabili come quei dati rientranti nelle "categorie particolari di dati personali" di cui all'art. 9 del GDPR e nonché qualificabili quali "dati personali relativi a condanne penali e reati" di cui all'art.

10 GDPR. La differenza lessicale non è di poco conto considerata la rilevanza delle conseguenze derivanti da un trattamento, o peggio, da un incidente informatico, che coinvolga dati di particolare natura ex artt. 9 e 10 GDPR.

Fatta questa premessa, si evidenzia, inoltre come sia alquanto complesso immaginare dati trattati da un PSP che non siano considerabili dati personali. Stiamo infatti parlando di informazioni derivanti da un conto di pagamento bancario e dal quale pare molto semplice poter dedurre informazioni di natura personale. Si ritiene quindi che il GDPR sia sempre applicabile ai PSP ma anche a tutti i cloud service provider esterni e aggregatori di API esterni che gestiscono per uno o più PSP, i sistemi di interfaccia alle diverse API delle varie banche o istituti di pagamento.

Passando all'analisi della PSD2, notiamo come l'art. 4(32) della direttiva comunitaria, dia una ulteriore definizione di dati sensibili, introducendo la figura dei "***dati sensibili relativi ai pagamenti***". Secondo tale articolo, si tratta di "*dati che possono essere usati per commettere frodi, incluse le credenziali di sicurezza personalizzate*." L'articolo poi prosegue precisando che "Per l'attività dei prestatori di servizi di disposizione di ordine di pagamento e dei prestatori di servizi di informazione sui conti, il nome del titolare del conto e il numero del conto non costituiscono dati sensibili relativi ai pagamenti".

Il perimetro normativo fornito dalla PSD2 in tema di dati personali e, in particolare, di dati "sensibili" è certamente carente rispetto a quanto, in maniera più completa ed esaustiva, viene definito nel GDPR.

Si ritiene quindi che, partendo dalla considerazione sopra detta, un PSP e i soggetti che collaborano con lui per il trattamento dei dati personali, dovranno sempre considerare qualunque dato trattato quale dato personale ai sensi del GDPR e valutare, sempre ai sensi del GDPR, se (sia in ipotesi di trattamento, conservazione o incidente informatico) il dato interessato sia di particolare natura o attinente informazioni di carattere giudiziario, ai sensi degli artt. 9 e 10 GDPR.

c) L'attivazione delle procedure di sicurezza nelle ipotesi di incidente di sicurezza ai sensi delle linee guida EBA.

In caso di incidente informatico nell'ambito delle attività poste in essere da un PSP è altamente probabile (se non certo) che l'incidente vada ad impattare sui dati personali dell'interessato. Ciò determinerà l'attivazione di una serie di misure finalizzate a tutelare da una parte l'interessato e dall'altra a monitorare il titolare del trattamento e i soggetti da lui nominati quali responsabili esterni al trattamento ex art. 28 GDPR, al fine di delimitare il perimetro dell'incidente, verificarne l'ampiezza a livello europeo e quindi il rischio effettivo e nel contempo valutare l'idoneità del PSP e l'eventuale sospensione o peggio revoca della sua licenza (questo aspetto in capo alla Banca Centrale di riferimento).

Il monitoraggio dell'incidente informatico da un lato e il *data breach* dall'altro, sono interessate da due aree di regolamentazione che, in alcuni passaggi rischiano sovrapposizioni rilevanti.

Partiamo dalle fonti di riferimento. Per quanto attiene le procedure relative ad un incidente informatico che occorre ad un PSP dobbiamo avere riguardo a quanto previsto all'art. 96 della PSD2, in tema di notifica degli incidenti, il quale prevede quanto segue: *"[i]n caso di grave incidente operativo o relativo alla sicurezza, i prestatori di servizi di pagamento lo notificano senza indugio all'autorità competente dello Stato membro di origine del prestatore di servizi di pagamento. Se l'incidente incide o potrebbe incidere sugli interessi finanziari dei propri utenti di servizi di pagamento, il prestatore di servizi di pagamento informa senza indugio i propri utenti di servizi di pagamento dell'incidente e di tutte le misure a disposizione che possono adottare per attenuarne gli effetti negativi*".

Già in questo primo comma, notiamo la evidente analogia con gli artt. 33 e 34 del GDPR dove si regolamenta l'obbligo di notifica di una violazione dei dati all'autorità di controllo (33) e, se del caso (34) agli interessati. Le differenze, però sono rilevanti soprattutto se si considerano le pesanti sanzioni che possono derivare da una incorretta applicazione dei termini di notifica ex GDPR che dovrebbe, quantomeno per questa parte, fungere da driver di riferimento in questo processo.

Qui di seguito una sintesi delle diverse tempistiche:

IPOTESI IN CUI L'INCIDENTE INFORMATICO NON COINVOLGE INTERESSI FINANZIARI DEI PROPRI UTENTI E VIOLAZIONE DATI PERSONALI CHE POSSA PRESENTARE UN RISCHIO PER I DIRITTI E LE LIBERTA' DELLE PERSONE FISICHE

	PSD2	GDPR
Destinatario della notifica	Banca Centrale del paese dove il PSP è stato licenziato	Garante Privacy del paese ove opera il titolare del trattamento interessato dal Personal Data Breach
Termine	Senza indugio	Senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui il titolare ne è venuto a conoscenza.
Fonte normativa	Art. 96 (1) PSD2	Art. 33 (1) GDPR

IPOTESI IN CUI L'INCIDENTE INFORMATICO COINVOLGE INTERESSI FINANZIARI DEI PROPRI UTENTI E/O VIOLAZIONE DATI PERSONALI CHE POSSA PRESENTARE UN RISCHIO ELEVATO PER I DIRITTI E LE LIBERTA' DELLE PERSONE FISICHE

	PSD2	GDPR
Destinatario della notifica	Gli utenti	Gli interessati
Termine	Senza indugio	Senza ingiustificato ritardo.
Fonte normativa	Art. 96 (2) PSD2	Art. 34 (1) GDPR

Da quanto sopra, appare evidente la necessità di uniformare le procedure nelle ipotesi di incidente informatico in capo ad un PSP, onde evitare una sovrapposizione di termini e soprattutto di procedure.

Si suggerisce, pertanto, innanzitutto di fare riferimento ai termini di cui al GDPR in modo da effettuare una unica comunicazione sia al Garante Privacy che alla Banca Centrale. E infatti, mentre il termine "senza indugio" appare generico, il termine di 72 ore (salvi casi motivati) appare quale termine inderogabile decorso il quale si può incorrere in rilevanti sanzioni. Un eventuale termine più lungo per la notifica alla Banca Centrale di riferimento potrebbe essere in effetti ammissibile pur sempre nel ragionevole lasso temporale consentito dal generico richiamo normativo e considerate le probabili diverse informazioni a cui potrebbe essere interessata la Banca Centrale.

Considerato che non viene dato un più preciso dettaglio concernente le procedure interne per la rilevazione e successiva segnalazione dell'incidente informatico, nonché per il contenuto della notifica (diversamente da

quanto previsto all'art. 33, comma 3 GDPR), viene lasciato un interessante spazio ai titolari e responsabili del trattamento, in ossequio al più generale principio di *accountability*, per meglio regolamentare tali passaggi.

Si ritiene quindi importante predisporre:

- una unica procedura comune sia in caso di incidente informatico di sicurezza che nelle ipotesi di personal data breach;
- un unico documento che accorpi entrambe le procedure;
- una attribuzione di compiti all'"*Incident response Team*" e al DPO in modo tale che entrambi, di concerto, valutino l'ampiezza dell'incidente e del breach, verifichino i potenziali soggetti interessati e la rilevanza degli interessi coinvolti, gestiscano la predisposizione delle bozze di notifica, si attivino per poi procedere al successivo invio, e gestiscano tutto il follow-up con Garante Privacy e Banca Centrale di riferinento nonché con gli interessati.

d) La gestione della valutazione di impatto sui rischi alla luce della PSD2 e del GDPR.

Un altro interessante punto di congiunzione tra PSD2 e GDPR può essere quello relativo alla valutazione dei rischi di cui al punto 3 delle LINEE GUIDA EBA/GL/2017/17 ("**Linee Guida EBA**") e la valutazione di impatto di cui all'art. 35 GDPR (DPIA).

Le Linee Guida EBA affrontano la valutazione dei rischi all'Orientamento n.3, concernente la individuazione delle funzioni, dei processi e delle risorse. Al punto 3.1, si stabilisce, in particolare, quanto segue: "*I prestatori di servizi di pagamento dovrebbero individuare, definire e aggiornare periodicamente un inventario delle funzioni aziendali, dei ruoli fondamentali e dei processi di supporto, al fine di identificare l'importanza di ciascuna funzione, ruolo e processo di supporto, nonché le loro interdipendenze in materia di rischi operativi e di sicurezza*".

Il punto 3.2, prosegue poi stabilendo quanto segue "*I prestatori di servizi di pagamento dovrebbero individuare, definire e aggiornare periodicamente un inventario delle risorse informatiche, come i sistemi ICT, le loro configurazioni, altre infrastrutture nonché le interconnessioni con altri sistemi interni ed esterni, per poter gestire le risorse che supportano le funzioni e i processi aziendali critici*".

L'Orientamento 3, ribadisce molto chiaramente (come peraltro richiamato in Italia nelle Disposizioni di Banca d'Italia del 29 luglio 2019) che, in quanto parte dell'obbligo di condurre e fornire alle autorità competenti una valutazione aggiornata e approfondita dei rischi operativi e di sicurezza relativi ai servizi di pagamento che prestano e dell'adeguatezza delle misure di mitigazione e dei meccanismi di controllo messi in atto per affrontarli (come previsto dall'articolo 95, paragrafo 2, della PSD2), i prestatori di servizi di pagamento dovrebbero eseguire e documentare, almeno su base annua, o a intervalli più ravvicinati determinati dall'autorità competente, valutazioni dei rischi delle funzioni, dei processi e delle risorse informatiche che hanno individuato e classificato come rilevanti ai fini dei principali rischi operativi e di sicurezza. Tali valutazioni dei rischi dovrebbero essere eseguite anche prima che sia attuata qualsiasi modifica sostanziale delle infrastrutture, dei processi o delle procedure tale da pregiudicare la sicurezza dei servizi di pagamento.

Sulla base delle valutazioni dei rischi, i prestatori di servizi di pagamento dovrebbero stabilire se e in quale misura sia necessario modificare le misure di sicurezza esistenti, le tecnologie utilizzate e le procedure o i servizi di pagamento offerti. I prestatori di servizi di pagamento dovrebbero tenere conto del tempo necessario per mettere in pratica le modifiche e del tempo necessario per adottare adeguate misure di

sicurezza provvisorie per ridurre al minimo gli incidenti operativi o di sicurezza, le frodi e potenziali impatti dirompenti per la prestazione dei servizi di pagamento.

Orbene, come noto, l'art. 35 del GDPR, in tema di valutazione di impatto sulla protezione dei dati, stabilisce che: "*Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi*".

Da quanto sopra, appare evidente come l'attività del PSP, sia per la natura dei dati trattati, per le finalità e per la probabile "larga scala", implichi necessariamente una valutazione di impatto preventiva (o DPIA). La DPIA sarà comunque svolta anche in ossequio a quanto indicato nell'orientamento n. 3 delle citate Linee Guida EBA e potrà quindi essere **ottimizzato il lavoro** con il coinvolgimento sia degli esperti in materia informatica e che hanno partecipato alla realizzazione della infrastruttura di riferimento e degli eventuali soggetti esterni (inclusi fornitori cloud e aggregatori di API per banche e istituti di pagamento).

Conclusioni

La presente ricerca ha evidenziato e comparato i **principali obblighi in materia di sicurezza** imposti dal GDPR, dalla Direttiva NIS e dalla PSD2. Queste tre normative hanno un impatto rilevante sui fornitori di servizi cloud: i cloud providers che trattano dati personali rientrano infatti all'interno della categoria di titolari/responsabili del trattamento; al contempo, sono considerati fornitori di servizi digitali e sono pertanto destinatari degli obblighi previsti dalla Direttiva NIS; inoltre, possono svolgere il ruolo di fornitori di servizi di pagamento (PISP) o di informazione su conti correnti bancari (AISP) ai sensi della PSD2.

Come chiarito, il **GDPR** impone di implementare misure di sicurezza tali da garantire un livello di sicurezza adeguato al rischio a cui sono esposti i dati personali affidando al contempo al titolare il compito di decidere in concreto quali misure applicare. Importanti obblighi di notifica (e di comunicazione) sono inoltre previsti in caso di violazione dei dati personali ai sensi degli articoli 33 e 34 GDPR. In questo contesto, l'articolo 28 GDPR gioca un ruolo fondamentale in quanto permette al titolare di mantenere il controllo sui dati ogni qual volta questi siano trattati per suo conto da soggetti terzi, ad esempio da soggetti eroganti servizi cloud.

Importanti obblighi in materia di sicurezza sono inoltre stati introdotti dalla **Direttiva NIS**, che mira a garantire un livello comune elevato di sicurezza delle reti e dei sistemi di informazione. I destinatari di tali obblighi sono, oltre agli operatori di servizi essenziali, i fornitori di servizi digitali, tra questi anche i fornitori di servizi cloud. La Direttiva NIS descrive infatti le misure di sicurezza che i fornitori di servizi digitali dovrebbero adottare per mitigare i rischi a cui la sicurezza della rete e dei sistemi informatici sono esposti e descrive la procedura di notifica degli incidenti informatici.

Da ultimo, la **PSD2** ha introdotto significative novità nel mondo dei pagamenti digitali. In primo luogo, la PSD2 ha introdotto tre nuovi player del settore, ovvero gli AISP, i PISP e i CISP ("PSP"). Per potere operare come PSP, tali soggetti dovranno superare le valutazioni delle Banche Centrali rispetto alle procedure adottate in caso di incidente informatico e alla consistenza degli investimenti che la società intende effettuare in ambito di sicurezza informatica. In particolare, un dettagliato quadro su come le società che intendono svolgere attività di PSP devono gestire gli incidenti informatici è descritto delle Guidelines dell'EBA del 27 luglio 2017. Inoltre, grande attenzione dovrà essere posta dai PSP alla protezione dei dati sensibili relativi ai pagamenti.

Nella pratica, gli obblighi previsti dal GDPR, dalla Direttiva NIS e quelli posti dalla PSD2 possono **parzialmente sovrapporsi**, pur mantenendo **oggetti di tutela differenti** e quindi **campi di applicazione diversi**. Vari punti di contatto possono infatti essere individuati tra le disposizioni in materia di sicurezza previste dalla NIS e dal GDPR anche se, nel complesso, gli obblighi di sicurezza sono descritti dalla NIS in modo più specifico e dettagliato rispetto al GDPR. Importanti sovrapposizioni possono inoltre interessare le procedure di notifica di *data breach* (ai sensi del GDPR) e di incidenti informatici (ai sensi della Direttiva NIS). Ulteriori sovrapposizioni potrebbero emergere tra il GDPR e la PSD2 dall'inquadramento dei PSP quale titolare/responsabile/co-responsabile del trattamento, dalla definizione di dato sensibile ai sensi della PSD2, dalle procedure da attivare in caso di incidente informatico, dalla gestione della valutazione d'impatto.

Al fine di superare eventuali problematiche gestionali che potrebbero emergere da queste sovrapposizioni, si rende opportuno gestire tali obblighi in maniera coordinata, procedendo ad esempio all'accorpamento della documentazione al fine di **ottimizzare** gli sforzi applicativi che le aziende sono chiamata ad affrontare.