GDPR INSIGHT

SERIES

PIPL vs GDPR

LA SVOLTA CINESE

NETPATROL

DATA PROTECTION & CYBER SECURITY

NET PATROL ITALIA

Net Patrol Italia è una società di consulenza specializzata in **privacy** e **cybersecurity**.

La nostra **squadra** è composta da consulenti specializzati in **privacy**, **information technology** e **cybersecurity**, in grado di affrontare in modo trasversale ogni questione e criticità.

La nostra metodologia di consulenza rispetta i principali **standard europei e internazionali**: FNCS, ENISA, NIST, oltre a tutte le linee guida dell'EDPB e delle Autorità competenti.

Per noi, privacy e cybersecurity sono **parte integrante** dei processi di business.

Il nostro obiettivo è quello di dare al cliente un **interlocutore unico,** in grado di affrontare la protezione dei dati con approccio multidisciplinare e **business oriented**.

Crediamo fermamente che privacy e cybersecurity siano due pilastri importanti dell'economia **data-driven**, oltre che un mezzo per **valorizzare e proteggere** il proprio business.

GDPR Insight è la serie di pubblicazioni a marchio Net Patrol con cui approfondiamo in modo semplice ma completo i temi che riguardano privacy e cybersecurity.

Ogni episodio della serie GDPR Insight è a cura dei nostri consulenti.

Se vuoi saperne di più sui servizi offerti da Net Patrol Italia, o se vuoi approfondire con noi gli argomenti trattati nelle nostre pubblicazioni, contattaci:

- **www.netpatrol.it**
- **info@netpatrol.it**
- **LinkedIn – Net Patrol Italia**

LA SVOLTA CINESE

Negli ultimi anni la Cina ha dato vita ad una vera e propria rivoluzione interna basata sulla data economy e sulla sovranità digitale.

Questo percorso ha recentemente preso una svolta, grazie a tre diverse leggi che creano tra loro un **framework comprensivo** ed esteso per tutto ciò che riguarda il trattamento di dati.

La prima di queste leggi è la **Cybersecurity Law**, entrata in vigore nel 2017.

Questa legge si propone di migliorare il livello di cybersicurezza nazionale, garantire la "sovranità del cyberspazio" e proteggere gli interessi nazionali.

La Cybersecurity Law si applica ad ogni ipotesi di costruzione, gestione e manutenzione di reti e infrastrutture. In questo senso, è **molto simile alla Direttiva NIS** entrata in vigore in UE nel 2016.

Alla Cybersecurity Law si agganciano poi due nuovi pezzi del puzzle, con implicazioni molto più estese e rilevanti per tutto il mondo – non solo per la Cina.

La prima è la **Data Security Law (DSL)**. La seconda è la **Personal Information Protection Law (PIPL)**.

L'applicazione di queste tre leggi, complementari tra loro, sarà prossimamente unificata e razionalizzata con un "**Network Data Security Management Regulation**" preparato dalla Cyberspace Administration of China (CAC), per ora in fase di consultazione pubblica.

Data Security Law (中华人民共和国数据安全法)

La Data Security Law (DSL) è in vigore in Cina dal **1° settembre 2021**.

Se da una parte la Cybersecurity Law del 2017 si occupa di definire le regole per assicurare un'adeguata sicurezza delle reti e dei sistemi di trattamento, la DSL si occupa invece di fornire alle aziende le regole e i principi a cui aderire per assicurare un **trattamento sicuro di dati personali e non-personali**.

La Data Security Law è quindi una legge che si occupa in modo specifico della sicurezza del trattamento dei dati.

Personal Information Protection Law (中华人民共和国个人信息保护法)

La Personal Information Protection Law (PIPL), in vigore dal **1° novembre 2021**, è la prima legge cinese specifica per quanto riguarda la definizione di regole armonizzate per il trattamento di dati personali.

La Cina è indubbiamente un colosso della tecnologia – anche più degli Stati Uniti e certamente più dell'Unione Europea. Essersi dotata di un **framework normativo specifico** per la protezione dei dati è quindi davvero un evento che impatta in tutto il mondo.

Lo scopo della PIPL è analogo a quello del **GDPR**: stabilire standard qualitativi per il trattamento di dati da parte delle aziende, rendere più efficiente il mercato attraverso la libera circolazione dei dati (data economy) e al tempo stesso proteggere i diritti dei cittadini contro possibili abusi.

Perché le aziende italiane dovrebbero interessarsi alle leggi cinesi?

Come per il GDPR, sia la PIPL che la DSL potranno applicarsi anche ad aziende stabilite al di fuori del territorio cinese, secondo alcuni criteri specifici.

Anche le aziende italiane che fanno affari con la Cina dovranno quindi rispettare questa normativa, proprio come le aziende fuori dall'UE devono rispettare il GDPR.

Le aziende che dal 2018 ad oggi hanno lavorato per implementare sistemi di gestione dei dati conformi al GDPR avranno certamente un margine competitivo rispetto alle altre.

Non bisogna però dormire sugli allori: un sistema conforme al GDPR non necessariamente sarà conforme anche a DSL e PIPL, perché queste leggi mantengono comunque le loro peculiarità e specificità.

In questo numero di GDPR Insight vedremo insieme le **principali caratteristiche della PIPL**, per aiutare le aziende a districarsi meglio in questa nuova sfida.

Net Patrol Italia srl — Via Napo Torriani 31, **Milano** | Via Molin Nuovo, 37/38, **Udine** - www.netpatrol.it

PIPL: CRITERI DI APPLICAZIONE

VEDIAMO COME E A CHI SI APPLICA LA PIPL

COME SI APPLICA LA LEGGE CINESE?

Come accennato nell'introduzione, vedremo insieme le principali caratteristiche della PIPL, la legge che più delle altre (Cybersecurity Law e Data Security Law) è destinata ad avere un impatto rilevante per chiunque faccia affari con la Cina.

Prima di tutto, bisogna capire qual è lo scopo di questa legge e come e quando si applica.

Lo scopo della Personal Information Protection Law (第一条)

Lo scopo della PIPL, descritto nell'articolo 1 della legge, è "proteggere i diritti delle persone, standardizzare le procedure di trattamento dei dati e promuovere un uso razionale dei dati".

L'obiettivo non è molto diverso da quello del GDPR. Anche la normativa europea ha come obiettivo primario quello di proteggere i diritti delle persone e standardizzare il trattamento di dati all'interno dell'Unione Europea. Ciò che manca invece al nostro GDPR è uno specifico riferimento all'uso "razionale" dei dati, che lascia intendere la volontà politica del governo cinese di determinare anche il modo in cui sono usati i dati.

I criteri di applicazione (第三条)

La legge si applica a **chiunque tratti dati personali**, sia all'interno del territorio cinese, che al di fuori.

Possiamo quindi dire che la PIPL si applica ad ogni soggetto che in qualche modo acquisisce e tratta dati riferibili a persone fisiche presenti in Cina per finalità di business. Il legislatore cinese definisce questi soggetti come **personal information handler (个人信息处理者)**, che nel GDPR sono chiamati **data controller** o **titolari del trattamento**, in italiano.

La PIPL però, similmente al GDPR, ha anche **un'estensione extra-territoriale**. La legge si applica infatti anche a tutti quei **soggetti stabiliti al di fuori della Cina** che in qualche modo acquisiscono e trattano informazioni riferibili a persone fisiche presenti in Cina.

Per capire se la PIPL si applica anche al trattamento di dati fatto da aziende situate fuori dalla Cina, bisogna guardare ai **criteri di applicazione territoriale**.

La normativa cinese si applica alle aziende italiane se:

PERSONAL INFORMATION PROTECTION LAW – APPLICAZIONE EXTRA-TERRITORIALE	
	L'azienda fornisce prodotti o servizi a persone fisiche presenti in Cina.
	L'azienda analizza o valuta il comportamento di persone fisiche presenti in Cina.
	Altre circostanze specifiche definite da leggi o regolamenti amministrativi.

In pratica, le aziende italiane che svolgono attività o forniscono prodotti e servizi a persone fisiche presenti in Cina sono tenute a rispettare la PIPL.

Questo vale anche nel caso in cui le aziende italiane assumano il ruolo di "responsabile del trattamento" e di importatori di dati (in Italia o altrove) per conto di clienti stabiliti in Cina. In questo bisogna fare molta attenzione, perché nella definizione di trasferimento di dati rientra **anche l'accesso da remoto** (ad esempio, dall'Italia) a data situati fisicamente in Cina.

Trasferire dati fuori dalla Cina

Per trasferire dati al di fuori della Cina è però necessario **rispettare alcune specifiche condizioni** che rendono lecito il trasferimento. Diversamente dal GDPR, le condizioni di liceità previste dalla PIPL sono molto più specifiche e stringenti.

Per esportare lecitamente dati fuori dalla Cina è necessario prima di tutto rispettare almeno una delle seguenti precondizioni:

Consenso	Prima di trasferire dati al di fuori della Cina è necessario notificare il trasferimento alle persone e ottenere il loro consenso specifico.
Valutazione d'impatto	Prima di trasferire dati al di fuori della Cina è necessario anche sottoporre il trattamento a una valutazione d'impatto.

Già da questo si possono notare le prime differenze con il GDPR. Anche la normativa europea prevede dei requisiti specifici per il trasferimento di dati extra-UE, ma lascia alle aziende la libertà di valutare la rischiosità del trasferimento e la valutazione d'impatto non è sempre obbligatoria (anche se raccomandata).

Il motivo di questa scelta è politico: in Cina la **sovranità digitale** è un tema molto sentito, e il **trasferimento di dati al di fuori del territorio** è per questo sempre visto come un **trattamento ad alto rischio** per gli interessi nazionali.

Anche l'ottenimento del **consenso esplicito** delle persone è una forma di garanzia in più rispetto agli interessi delle persone (e dello Stato). Anche in questo il GDPR è leggermente diverso dalla PIPL, in quanto il consenso esplicito delle persone è richiesto soltanto in alcuni frangenti.

Ma oltre a queste due condizioni, sempre necessarie, è anche obbligatorio rispettare almeno una delle seguenti condizioni ulteriori:

Certificazione	Sottoporsi a una "personal information protection certification" condotta da un ente specializzato, secondo i requisiti previsti dal dipartimento di Stato per la Cybersecurity.
Security assessment	Gli operatori di infrastrutture critiche e titolari del trattamento che trattamento grandi quantità di dati devono sottoporsi a una valutazione di sicurezza fatta dal dipartimento di Stato per la Cybersecurity.
Contratto	Concludere un contratto con l'importatore di dati contenente delle clausole standard formulate dal dipartimento di Stato per la Cybersecurity.
Leggi e regolamenti	In alcuni casi sono altre leggi e regolamenti amministrativi specifici che prevedono condizioni particolari per autorizzare il trasferimento di dati al di fuori della Cina.

La certificazione non è espressamente disciplinata dalla PIPL, che, come il GDPR, rimanda a successivi atti e schemi di certificazione. Fra qualche mese magari sapremo meglio in cosa consiste.

La differenza più marcata, che rispecchia in tutto lo spirito della Cina, è forse **l'obbligo di security assessment** per gli operatori di infrastrutture critiche (CIIOs) e per i titolari del trattamento che gestiscono grandi quantità di dati. Se è vero quanto detto finora, cioè che i dati sono un asset strategico nazionale, è anche facile comprendere il motivo di questa disposizione. In questo probabilmente l'UE potrebbe imparare qualcosa.

Infine, rimangono le ultime due ipotesi: il **contratto tra esportatore e importatore**, e specifiche disposizioni di legge. Come per il GDPR, anche la PIPL prevede la possibilità di trasferire dati al di fuori del territorio in presenza di specifiche clausole contrattuali sottoscritte tra le parti.

PRINCIPI GENERALI

I PRINCIPI DELLA PIPL E COSA CAMBIA RISPETTO AL GDPR

PRINCIPI GENERALI (第一章 总 则)

Come anticipato, la PIPL non è molto diversa dal GDPR, pur mantenendo alcune peculiarità. Proprio come nel caso del GDPR, anche la PIPL descrive alcuni principi fondamentali e condizioni di liceità da rispettare ogni volta che si trattano dati personali.

Diversamente dal GDPR, i principi del trattamento sono descritti in più articoli (dal 5 al 12), vediamo insieme quali sono.

I principi fondamentali (第五条)

L'articolo 5, molto breve, descrive i principi fondamentali che dovrebbero ispirare ogni trattamento di dati:

- Legittimità
- Legalità
- Necessità
- Buona fede

Oltre a questi principi, è espressamente affermato che è **vietato trattare dati personali in modo coercitivo, ingannevole, o con raggiri**.

Questo è particolarmente interessante perché potrebbe essere un principio richiamato in caso di utilizzo di "**dark patterns**", che invece il GDPR fatica a coprire (se non attraverso interpretazione estensiva).

Limitazione delle finalità e minimizzazione (第六条)

Il seguente articolo 6 ci riporta a questioni più concrete, affermando che il trattamento di dati personali deve avere uno **scopo chiaro e ragionevole** e deve avere una **connessione diretta** con il motivo per cui i dati sono acquisiti.

La norma può essere interpretata in modo simile al **principio di limitazione delle finalità** del GDPR, anche se sembrerebbe suggerire un approccio ancora più restrittivo.

Secondo il GDPR il trattamento di dati deve essere **compatibile con le finalità** per cui i dati sono stati raccolti. Ma se nel GDPR questo giudizio di compatibilità viene lasciato al Titolare, nella PIPL sembrerebbe necessario dimostrare un **nesso causale diretto** tra acquisizione e seguente trattamento dei dati.

Una differenza ancora più interessante riguarda il principio di minimizzazione.

Il trattamento di dati personali, infatti, oltre a dover rispettare il principio di minimizzazione che conosciamo grazie al GDPR (acquisire e trattare solo i dati strettamente necessari) deve anche essere fatto in modo tale da avere il **minor impatto possibile** sui diritti e interessi delle persone.

Una sorta di **principio di minimizzazione rafforzato**.

Trasparenza (第七条)

Il principio di trasparenza è pressoché identico a quello previsto dal GDPR. Non dovrebbero esserci grossi problemi di interpretazione, come vedremo poi nel paragrafo dedicato alla privacy policy.

Qualità dei dati (第八条)

Il GDPR ci dice che i dati devono essere adeguati, pertinenti, esatti e se necessario aggiornati.

La PIPL afferma invece che i data handler devono a**ssicurare la qualità dei dati personali** ed evitare rischi per i diritti e interessi delle persone derivanti dall'uso di dati inaccurati e o incompleti.

Anche in questo caso, pur affermando sostanzialmente gli stessi principi, traspare la natura più prescrittiva e meno astratta della PIPL, che lo fa diventare un vero e proprio obbligo esplicito.

Accountability (第九条)

Anche per la PIPL chi tratta dati personali deve assumersene ogni responsabilità, e deve assicurare **l'adozione di ogni misura necessaria per garantire la sicurezza delle informazioni trattate**.

Da questo punto di vista non ci sono molte differenze con il GDPR, e tutto il framework normativo conferma lo stesso approccio.

L'impegno esplicito dello Stato

Una netta differenza con il GDPR si percepisce nella conclusione del capitolo sui principi generali.

L'articolo 11 in particolare si rivolge direttamente allo Stato, e sembra quasi una proclamazione d'intenti: lo Stato si impegna espressamente a stabilire una struttura (fatta anche di leggi) per garantire la protezione delle informazioni personali e per prevenire e punire qualsiasi atto che possa danneggiare i diritti e gli interessi delle persone.

Ma non solo, lo Stato si impegna anche a migliorare le condizioni di trattamento con **attività di propaganda e educazione in materia di protezione dei dati** e anche a promuovere un "buon contesto sociale" attraverso la collaborazione del governo, delle aziende, delle organizzazioni sociali e del pubblico.

Un altro importante segnale delle differenze "politiche" tra GDPR e PIPL arriva dall'articolo 62, che prevede le competenze del CAC (Cyberspace Administration of China). Tra queste spiccano la formulazione di **regole e standard specifici** per la protezione dei dati, per le piccole imprese, e per alcune tecnologie innovative (come l'intelligenza artificiale). In questo senso torna prevalente lo scopo esplicito della PIPL: **razionalizzare** e standardizzare il trattamento di dati.

Le condizioni di liceità del trattamento (第十三条)

Come visto, tra i principi generali c'è la "legalità" del trattamento. Questa fa riferimento al rispetto di specifiche disposizioni di legge che prescrivono **le condizioni da rispettare per avere un trattamento lecito** di dati.

Vediamo insieme le differenze tra le due normative per quanto riguarda le condizioni di liceità, nell'ordine in cui sono proposte dai rispettivi articoli:

GDPR (ARTICOLO 6)	PIPL (ARTICOLO 13)
Consenso del soggetto interessato.	Consenso del soggetto interessato
Trattamento necessario all'esecuzione di un contratto o esecuzione di misure precontrattuali.	Trattamento necessario alla conclusione o esecuzione di un contratto o necessario all'esecuzione di attività di gestione delle risorse umane, nel rispetto delle normative di settore sul diritto del lavoro e dei contratti collettivi.
Trattamento necessario a adempiere a un obbligo legale.	Trattamento necessario a adempiere a un obbligo legale.
Trattamento necessario per la salvaguardia di interessi vitali del soggetto interessato.	Trattamento necessario per rispondere a emergenze di salute pubblica, per proteggere la vita e salute delle persone, per proteggere la sicurezza della loro proprietà o in caso di condizioni d'emergenza.
Trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri.	Per pubblicare notizie e inchieste e altre attività analoghe nel pubblico interesse.
Trattamento necessario per il perseguimento del legittimo interesse del Titolare o di terzi.	Quando le informazioni sono rese manifestamente pubbliche dalla persona, per finalità ragionevoli e nel rispetto della legge.
/	Altre circostanze previste da leggi e regolamenti amministrativi specifici.

Le condizioni di liceità del trattamento di dati sensibili (敏感个人信息的处理规则)

La PIPL dedica un'intera sezione del Capitolo 2 alle condizioni di liceità per il trattamento di dati sensibili.

La grande differenza rispetto al GDPR, è che la PIPL fornisce una **definizione molto più ampia** e astratta dei dati sensibili.

I DATI "SENSIBILI" SECONDO LE DUE NORMATIVE	
GDPR (articoli 4, 9)	**PIPL (articoli 28, 29)**
Dati sensibili ("particolari") sono quelle informazioni che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religione o filosofiche, l'appartenenza sindacale. Sono anche dati particolari i dati genetici, biometrici, relativi allo stato di salute, alla vita sessuale o all'orientamento sessuale della persona.	Dati sensibili sono quelle informazioni che, se diffuse o usate in modo illecito, possono causare un danno alla dignità della persona o danni biologici o al suo patrimonio. Tra queste informazioni sono comprese quelle relative a caratteristiche biometriche, convinzioni religiose, stati particolari, relative allo stato di salute. Nel novero dei dati sensibili rientrano anche espressamente informazioni che riguardano lo stato finanziario delle persone, i dati di geolocalizzazione, e le informazioni che riguardano i minori di 14 anni.

Come è facile vedere, il novero dei dati "sensibili" previsto dalla PIPL è molto più ampio di quello del GDPR, che fornisce un elenco tassativo e abbastanza ristretto di dati sensibili (chiamati dati particolari).

L'elenco dell'articolo 28 PIPL non è invece tassativo, in quanto le tipologie indicate sono soltanto a titolo esemplificativo. Starà quindi ai data handler **valutare il livello di sensibilità dei dati** nel caso concreto.

Una grave lacuna del GDPR è il non aver incluso i dati finanziari nel novero dei dati particolari. Una diffusione di dati finanziari, insieme a dati di contatto, pone infatti gravi rischi per il patrimonio delle persone (truffe, phishing, estorsioni, ecc.). Lo stesso discorso vale certamente per i dati che riguardano i minori.

L'effetto di queste differenze, per le aziende italiane a cui si applica la normativa cinese, è che dovranno proteggere dati considerati comuni in UE, come quelli finanziari o quelli sulla geolocalizzazione, come se fossero dati particolari – alla stregua dei dati relativi allo stato di salute.

Un'ulteriore differenza è che la PIPL prevede che i dati sensibili possano essere trattati **solo con il consenso delle persone**, mentre il GDPR prevede ben 9 condizioni di liceità diverse dal consenso.

Privacy policy (第十七条)

Prima di raccogliere dati personali, i data handler sono tenuti a fornire ai soggetti interessati tutte le **informazioni** che riguardano il trattamento, usando un linguaggio chiaro e facilmente comprensibile.

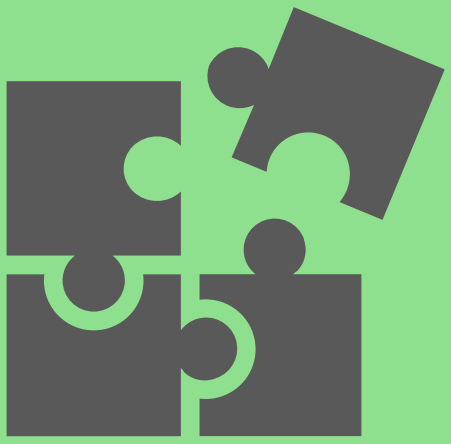
In particolare, devono essere fornite almeno le seguenti informazioni:

- Dati di contatto del data handler
- Finalità e modalità del trattamento
- Categorie di dati e tempi di conservazione
- Modalità di esercizio dei diritti
- Altre informazioni richieste da leggi specifiche

Ciò che le aziende italiane dovranno valutare sarà **la lingua in cui pubblicare le privacy policy**. La legge infatti richiede che sia usato un linguaggio facilmente comprensibile, e l'inglese potrebbe non essere considerato tale, rispetto al cinese.

GOVERNANCE

LA GESTIONE DEI DATI E DELLA CONFORMITÀ



GOVERNANCE DEI DATI (个人信息处理者的义务)

Anche la PIPL, come il GDPR, prevede specifiche disposizioni che riguardano la gestione interna dei dati e della conformità alla legge.

Sistema di gestione (内部管理制度和操作规程)

Una prima disposizione riguarda primariamente la definizione di un sistema di gestione interno, uno dei cardini del principio di **accountability**.

In questo, le aziende italiane già conformi al GDPR non dovrebbero avere molte difficoltà. Anche la normativa europea incentiva lo sviluppo di un **sistema di gestione interno** che possa garantire il rispetto dei requisiti di legge e di poterlo dimostrare.

Ciò che differisce è la **maggiore specificità** della norma cinese, che prevede alcuni obblighi non espressamente previsti dal GDPR:

1	Adottare procedure e politiche interne per la gestione dei dati
2	Adottare un sistema di categorizzazione dei dati trattati (come il Registro del trattamento)
3	Implementare misure di sicurezza tecniche come crittografia e de-identificazione
4	Individuare i limiti di trattamento interni, formare e sensibilizzare i dipendenti
5	Formulare e implementare piani di risposta agli incidenti di sicurezza
6	Altre misure specificatamente indicate dalla legge

Tra le principali differenze rispetto al GDPR spicca sicuramente **l'obbligo di formazione** e sensibilizzazione dei dipendenti.

Il GDPR all'articolo 29 prescrive che il titolare debba **istruire** i dipendenti che trattano dati, ma c'è una grande differenza tra il dare delle istruzioni da seguire e organizzare un programma di formazione e sensibilizzazione.

Per quanto riguarda invece l'adozione di **procedure e politiche interne** per la gestione dei dati, la differenza con il GDPR sta nell'obbligo.

Secondo la PIPL **ogni data handler deve adottare politiche e procedure per la gestione dei dati**, mentre nel GDPR queste devono essere adottate solo quando "proporzionato" rispetto alle attività di trattamento.

Un'azienda italiana a cui si applica la PIPL dovrebbe fare quindi attenzione a queste differenze.

In caso di **audit** da parte delle autorità o di clienti cinesi, l'azienda dovrebbe infatti essere nelle condizioni di **dimostrare di aver compiuto attività anche non richieste espressamente dal GDPR**, come la formazione dei dipendenti o l'adozione di politiche per la gestione dei dati.

Audit (合规审计)

La PIPL obbliga esplicitamente i data handler a sottoporsi ad **audit periodici** relativi per la verifica della conformità delle attività di trattamento.

Questo aspetto non è formalmente regolato dalla normativa europea, anche se all'articolo 24 è previsto che il titolare del trattamento debba riesaminare e aggiornare le misure organizzative e tecniche interne quando necessario.

Più che a un audit vero e proprio, il richiamo del GDPR è più vicino all' attività di monitoraggio e miglioramento continuativo del sistema di gestione interno.

La differenza tra quanto previsto dalla PIPL e dal GDPR è ulteriormente confermata dal fatto che nella PIPL l'autorità può **obbligare le aziende a sottoporsi ad audit di terza parte** nel caso di trattamenti ad alto rischio.

Personal Information Impact assessment (信息保护影响评估)

Anche la PIPL ha previsto un meccanismo simile alla valutazione d'impatto (DPIA) previsto dal GDPR.

Lo scopo è lo stesso: facilitare l'identificazione e la valutazione dei rischi che derivano dal trattamento di dati personali e valutare l'adozione di misure di mitigazione adeguate.

La valutazione d'impatto è **obbligatoria** in alcuni casi:

1	Quando si trattano dati sensibili
2	Quando si trattano dati nell'ambito di processi decisionali automatizzati
3	Quando il trattamento di dati è delegato a terzi o quando i dati sono devono essere pubblicamente
4	Quando c'è un trasferimento di dati fuori dalla Cina
5	Quando il trattamento ha un impatto significativo sui diritti delle persone

La **normativa europea** prevede invece un obbligo di DPIA quando un trattamento può presentare un **rischio elevato** per i diritti e le libertà delle persone, oltre ad alcuni casi specifici previsti dall'articolo 35 e dai provvedimenti nazionali delle Autorità (provv. 467/2018 in Italia).

Da queste differenze potrebbero derivare anche **alcune asincronie** tra l'obbligo di valutazione d'impatto ai sensi del GDPR e della PIPL.

Ad esempio, il trattamento di dati relativi alla **geolocalizzazione** (anche online) in applicazione della PIPL richiederebbe una valutazione d'impatto a prescindere (essendo considerato dato sensibile), mentre in Italia questa sarebbe obbligatoria solo se effettuata su larga scala (ai sensi del provv. 467/2018).

La valutazione d'impatto deve contenere almeno le seguenti informazioni:

- Valutazione di legittimità e necessità delle finalità e modalità del trattamento di dati
- Impatto sui diritti e interessi delle persone e rischi di sicurezza
- Indicazione delle misure di mitigazione adottate e della loro adeguatezza

Una novità, rispetto al GDPR, è l'obbligo di **mantenere la documentazione** relativa alle valutazioni d'impatto per **almeno 3 anni**.

In questo senso si consacra il valore della valutazione d'impatto anche come strumento per **dimostrare il livello di accountability** del data handler.

Responsabili del trattamento (个人信息的受托人)

Un elemento essenziale di governance, anche per la PIPL, è il rapporto tra data handler (titolare del trattamento) e i soggetti **fiduciari (个人信息的受托人)** a cui viene assegnato un trattamento di dati, che nel linguaggio del GDPR vengono definiti "Responsabili del trattamento".

Anche la normativa cinese impone la conclusione di un **contratto** tra le parti attraverso il quale disciplinare:

- Le finalità del trattamento
- Il limite temporale del trattamento affidato
- Le categorie di dati interessate
- Le misure di sicurezza
- Gli obblighi e diritti delle parti

E come per il GDPR, il data handler ha l'onere di **supervisionare** le attività del soggetto a cui sono affidate le attività di trattamento di dati.

Allo stesso tempo, i fiduciari hanno l'obbligo di adottare tutte le misure necessarie per garantire la sicurezza dei dati e **collaborare con il data handler** per adempiere agli obblighi di legge.

Vale la pena sottolineare che anche un'azienda italiana potrebbe essere un soggetto "fiduciario" per conto di un data handler cinese, ad esempio nel caso di **Software as a Service** venduto in licenza ad aziende cinesi, ma gestito da software house italiana.

Data breach (第五十七条)

La regolamentazione degli eventi di data breach prevede **tre elementi** principali:

- L'adozione di misure di ripristino e mitigazione delle conseguenze
- La notifica alle autorità competenti
- La notifica ai soggetti interessati

La sostanziale differenza tra GDPR e PIPL è nella **gestione della notifica** di data breach.

Come sappiamo, il GDPR lascia ampio spazio interpretativo sulla scelta di notificare o meno il data breach (sia all'Autorità competente che ai soggetti interessati). Il motivo è che nel framework del GDPR è sempre **centrale il concetto di rischio**, che però deve essere valutato dal titolare in base al caso concreto.

Il legislatore cinese ha invece deciso di **eliminare questa incertezza**, preferendo un approccio più prescrittivo e pragmatico (come in altri casi già evidenziati).

Vediamo quindi quali sono le differenze tra PIPL e GDPR nella gestione del data breach:

NOTIFICA DI DATA BREACH			
GDPR (ARTT. 33-34)		**PIPL (ART. 57)**	
Termini	Entro 72 ore dalla scoperta	**Termini**	Immediatamente
Contenuto	▪ Natura della violazione ▪ Categorie e numero dei soggetti interessati ▪ Categorie e numero dei dati ▪ Dati di contatto del DPO o del titolare ▪ Descrizione delle conseguenze ▪ Descrizione delle misure di mitigazione adottate	**Contenuto**	▪ Cause della violazione ▪ Categorie di dati ▪ Descrizione delle conseguenze ▪ Descrizione delle misure di mitigazione adottate ▪ Dati di contatto del data handler
Quando notificare all'Autorità	Sempre, salvo che sia improbabile che la violazione presenti un rischio per i diritti e libertà delle persone.	**Quando notificare all'Autorità**	Sempre, anche se non c'è completa certezza della violazione.
A chi notificare	All'Autorità competente a norma dell'articolo 55 o al titolare del trattamento (per i responsabili).	**A chi notificare**	Cyberspace Informatization Department (CAC) / dipartimenti di Stato competenti in base a specifica regolamentazione.
Quando notificare ai soggetti interessati	Quando la violazione è suscettibile di presentare un rischio elevato per diritti e libertà delle persone.	**Quando notificare ai soggetti interessati**	Sempre, salvo aver adottato misure in grado di evitare le conseguenze negative della violazione.

L'approccio cautelativo del legislatore cinese è tale che prevede **l'obbligo di notifica** anche nel caso in cui sia **soltanto probabile** che il data breach sia avvenuto. Per far scaturire l'obbligo di notifica è quindi sufficiente il dubbio di essere stati vittima di un incidente.

Questo approccio mostra l'importanza dei dati per la Cina. Una violazione di dati non è soltanto un incidente di percorso, ma un vero e proprio evento che mette in pericolo la **sovranità digitale della nazione**, e che pertanto deve essere sempre notificato.

SANZIONI E CONSIGLI

QUALI SONO LE SANZIONI, E COME EVITARLE

LE SANZIONI, E ALCUNI CONSIGLI PER EVITARLE

Le sanzioni (第五十七条)

Trattare dati personali in violazione della PIPL può comportare l'erogazione di sanzioni amministrative, proprio come il GDPR. Ci sono due livelli sanzionatori, in base alla gravità delle circostanze.

Diversamente dal GDPR, le sanzioni pecuniarie sono erogate anche alle **persone fisiche direttamente responsabili della violazione**, ad esempio persone in ruoli apicali o a cui sono state delegate specifiche funzioni di gestione della conformità alla PIPL.

SANZIONI	
VIOLAZIONI NON GRAVI	**VIOLAZIONI GRAVI**
In caso di violazioni non gravi, le autorità possono: ■ emettere provvedimenti correttivi ■ confiscare guadagni illeciti ■ sospendere il servizio ■ sanzionare le persone direttamente responsabili fino a un massimo di €14.000 (circa)	In caso di violazioni gravi, le autorità possono: ■ emettere provvedimenti correttivi ■ confiscare guadagni illeciti ■ sospendere le attività dell'azienda e/o revocare licenze e permessi ■ sanzionare l'azienda fino a € 7.000.000 (circa) o 5% del fatturato annuale ■ sanzionare le persone direttamente responsabili fino a un massimo di €140.000 (circa) ■ divieto di assumere posizioni apicali (direzione, manager, personal information protection officer)

Oltre alle sanzioni pecuniarie verso l'azienda e verso le persone responsabili della violazione, di particolare interesse è la possibilità di **sospendere l'attività dell'azienda o revocare licenze e permessi** – un'eventualità che potrebbe mettere in seria difficoltà le aziende.

Alcuni consigli per affrontare la PIPL

In generale, un'azienda con un buon sistema di gestione per la conformità al GDPR non dovrebbe avere grandi problemi, ricordando comunque che un adeguamento è necessario a causa di alcune marcate differenze.

Vediamo **qualche consiglio operativo** per affrontare la PIPL:

- Valutare attentamente le basi giuridiche per il trattamento, tenendo conto in particolare delle **differenti definizioni di dati sensibili** (particolari) tra le due normative
- Se necessario, **integrare informative privacy** almeno in lingua inglese (preferibilmente in lingua cinese)
- Implementare politiche e procedure aziendali interne per **gestire gli eventi rilevanti**, come i data breach
- **Integrare la DPIA** nei processi aziendali per ogni ipotesi prevista obbligatoriamente dalla PIPL
- Massima attenzione ai **trasferimenti di dati al di fuori dalla Cina** – questo comprende anche l'accesso da remoto a data center e database fisicamente situati in Cina
- Organizza **programmi di formazione** e sensibilizzazione per management e dipendenti
- Mantieni traccia delle **decisioni e azioni** nell'ambito del sistema di conformità, ai fini probatori

Per il resto, se hai dubbi sulla conformità del tuo sistema alla PIPL, prova a **chiedere consiglio al tuo DPO** o al tuo consulente privacy.

NET PATROL ITALIA

PRIVACY | CYBERSECURITY | DPO

www.netpatrol.it - info@netpatrol.it - 02 87165913

Sede di Milano
Via Napo Torriani, 31 | Milano

Sede di Udine
Via Molin Nuovo, 37/38, Udine

GDPR INSIGHT SERIES, N° 7

PIPL vs GDPR, LA SVOLTA CINESE

Dicembre 2021

Disclaimer:

Questa pubblicazione non intende sostituire le fonti legali e riflette unicamente le opinioni degli autori.

Le azioni intraprese dalle organizzazioni non possono basarsi esclusivamente sulla lettura di questa pubblicazione.

In nessun modo la lettura di questa pubblicazione può sostituire il lavoro prestato da persone specializzate e competenti nella materia della protezione dei dati personali. Net Patrol Italia s.r.l. non può essere ritenuta responsabile per i danni o le violazioni del Regolamento UE 2016/679 o altra normativa rilevante realizzate dalle organizzazioni che fondino le proprie decisioni esclusivamente sulla base di questa pubblicazione.