
“Dietro ogni problema c’è un’opportunità”
Galileo Galilei

talleri law

GDPR & OUTSOURCING

Outsourcing: i dati sensibili gestiti dalla mia azienda sono davvero al sicuro?

Il GDPR come strumento per (ri)appropriarsi del controllo di una risorsa fondamentale.

1. **GDPR?**
   Breve introduzione al GDPR
2. **CH & GDPR?**
   Portata del GDPR per la Svizzera
3. **TRATTAMENTO DEI DATI**
   Nell'ottica di attività in outsourcing
4. **SOLUZIONI?**
   Identificare le criticità con l'analisi dei contratti
5. **DOMANDE**

GDPR (anche) per la FIDUCIA

quale premessa per lo sviluppo del mercato interno

25 maggio 2018; una nuova era nell'ambito della protezione dei dati, entra in vigore il GDPR.

Fra gli obiettivi perseguiti dal Regolamento vi è quello "*di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno. È opportuno che le persone fisiche abbiano il controllo dei dati personali che li riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche*".

Il GDPR (anche) come strumento di promozione dello sviluppo commerciale all'interno dell'EU.

Il GDPR in breve

Regolamento Generale sulla Protezione dei Dati

- Entrato in vigore il 24 maggio 2016 (!) e
- efficace **da oggi, 25 maggio 2018**;
- **99** articoli e **173 (!)** considerandi;
- Regolamento **unico per l'Unione Europea**;
- Nuovi strumenti per attuare **principi già esistenti**:
- **Liceità, correttezza e trasparenza**;
- **Limitazione** della finalità;
- **Limitazione** della conservazione;
- **Minimizzazione dei dati**;
- **Esattezza** dei dati;
- **Integrità e riservatezza**;
- **Responsabilizzazione**.

IL MINIMO DEI DATI NECESSARI, ESATTI, LEGALI, INTEGRI E RISERVATI, CUSTODITI ADEGUATAMENTE.

Perché il GDPR spaventa?

…. forse eccessivamente …

- **sanzioni pecuniarie** fino ad un massimo di € 20.000.000 oppure, per le imprese, fino al 4% del fatturato mondiale totale annuo riferito all'esercizio precedente;
- misure amministrative;
- **responsabilità personali**;
- obbligo di documentazione;
- **inversione onere probatorio.**

I diversi Stati dell'EU stanno adeguando il diritto interno al GDPR, ma la portata effettiva di talune norme la si avrà solo quando si svilupperà al riguardo della giurisprudenza; NO PANIC!!!

… si, ma in Svizzera?

(in attesa della nuova Legge federale sulla protezione dei dati)

- **applicabilità del GDPR alla Svizzera: SI***
- **incertezza** circa l'applicazione delle sanzioni in Svizzera;
- il GDPR **implica la responsabilità personale dei responsabili aziendali**;
- espone al **rischio di procedure giudiziarie in EU**;
- pone **problematiche contrattuali**;
- **rischio concorrenziale e di mercato** (in caso di mancanza di compliance GDPR).

* vedi le condizioni alle slide successive

Il fatto che il GDPR torni in alcuni casi applicabile anche alla Svizzera quale stimolo per adeguarsi anche alla futura LPD; un'opportunità da cogliere.

GDPR e CH

APPLICAZIONE TERRITORIALE, art. 3 GDPR

Articolo 3
Ambito di applicazione territoriale

*1. Il presente regolamento si applica **al trattamento dei dati personali** effettuato nell'ambito delle attività di uno **stabilimento da parte di un titolare del trattamento** o di un responsabile del trattamento **nell'Unione**, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.*

*2. Il presente regolamento si applica **al trattamento dei dati personali di interessati che si trovano nell'Unione**, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:*
*a) **l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione**, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure*
*b) **il monitoraggio del loro comportamento** nella misura in cui tale comportamento ha luogo all'interno dell'Unione.*

3. Il presente regolamento si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico.

- **il titolare del trattamento o un suo responsabile ha stabilimento nell'EU (criterio dello stabilimento) indipendentemente da dove viene effettuato il trattamento;**
- **i beni e i servizi sono offerti all'interno dell'EU (criterio dell'individuazione);**
- **viene monitorato il comportamento di internauti residenti nell'EU.**

Outsourcing

risorsa e business aziendale

L'esternalizzazione, anche detta outsourcing,
(parola inglese traducibile letteralmente come "approvvigionamento esterno")
è in economia e organizzazione aziendale, l'insieme delle pratiche adottate dalle imprese o dagli enti pubblici di ***ricorrere ad altre imprese per lo svolgimento di alcune fasi del proprio processo produttivo o fasi dei processi di supporto****.*
(fonte: Wikipedia)

Il GDPR, per i motivi brevemente illustrati in seguito, impone di garantire la tutela dei dati personali anche quando si ricorre ad un terzo per il loro trattamento. Di fatto questo impone di effettuare la verifica, fra le altre cose, della base contrattuale che regola tale trattamento. Non di rado tali basi sono desuete o addirittura definite per atti concludenti. Tale verifica si può estendere anche ad altri servizi (cloud, ecc.).

L'avvento del GDPR permette quindi di definire, a tutela dei dati personali gestiti dal titolare, ma anche a tutela di quest'ultimo, una base contrattuale chiara; di qui la grande opportunità offerta dal GDPR.

Figure centrali e trattamento

identificate dal GDPR quali attori del trattamento dei dati

Articolo 4 GDPR

*«**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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;*

***«responsabile del trattamento»:** è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (art. 4 cpv. 8);*

***«terzo»:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile (art. 4 cpv. 10).*

Articolo 29 GDPR

Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento (C81)
Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

TITOLARE e RESPONSABILE del trattamento quali parti del contratto.

Il responsabile del trattamento

Articolo 28 GDPR

Responsabile del trattamento

1. 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 del presente regolamento e garantisca la tutela dei diritti dell'interessato.

2. Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

*3. **I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli 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.***

- **il responsabile deve offrire garanzie;**
- **senza autorizzazione nessuna subdelega;**
- **trattamento disciplinato da un contratto.**

Contenuto del contratto

Articolo 28 cpv. 3 GDPR

Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:

*a) tratti i dati personali soltanto **su istruzione documentata del titolare** del trattamento (...)*
*b) **garantisca** che le persone autorizzate al trattamento dei dati personali si siano **impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;***
*c) adotti tutte le **misure** richieste ai sensi dell'articolo 32;*
d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;
*e) tenendo conto della natura del trattamento, **assista il titolare del trattamento con misure tecniche e organizzative adeguate**, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;*
*f) **assista il titolare del trattamento nel garantire il rispetto degli obblighi** di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;*
*g) su scelta del titolare del trattamento, **cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione** dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; e*
*h) metta a disposizione del titolare del trattamento **tutte le informazioni necessarie per dimostrare il rispetto** degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato. Con riguardo alla lettera h) del primo comma, il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.*

Il cpv. 3 dell'art. 28 GDPR non è un elenco esaustivo, ma offre una base solida sulla quale stipulare un contratto.

Contenuto del contratto

… inoltre…

Occorre che:

il responsabile che fa capo ad un altro responsabile si deve accertare che il contratto preveda per quest'ultimo gli stessi obblighi in materia di protezione dei dati, in caso contrario **«*il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile*» (art. 28 cpv. 4 GDPR).**

Attenzione:

il contratto (art. 28 cpv. 3 e 4 GDPR) **è stipulato in forma scritta** (vale anche il formato elettronico; art. 28 cpv. 10 GDPR).

- **Verifica in caso di subdelega;**
- **Forma scritta dei contratti.**

Privacy by design

la protezione dei dati come impostazione iniziale

Articolo 25 GDPR

Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (C75-C78)

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso 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.

2. 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. 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.

3. Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo.

Prima di offrire o richiedere prestazioni in outsourcing occorre quindi pianificare accuratamente quali dati è indispensabile trattare e in quali modi garantirne la protezione.

Sicurezza

Articolo 32 GDPR

Sicurezza del trattamento (C83)

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative ade- guate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) ***la pseudonimizzazione e la cifratura dei dati personali;***

b) ***la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza*** *dei sistemi e dei servizi di trattamento;*

c) ***la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico****;*

d) una ***procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative*** *al fine di garantire la sicurezza del trattamento.*

2. Nel valutare l'adeguato livello di sicurezza, ***si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso,*** *in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.*

3. L'adesione a un codice di condotta approvato di ***cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo****.*

4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

- **la pseudonimizzazione e la cifratura dei dati personali;**
- **assicurare su base permanente;**
- **valutare regolarmente;**
- **valutazione del rischio.**

Notifica

Articolo 33 GDPR

Notifica di una violazione dei dati personali all'autorità di controllo

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 ***senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche****. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.*

2. Il responsabile del trattamento ***informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.***

3. La notifica di cui al paragrafo 1 deve almeno:

a) ***descrivere la natura della violazione*** *dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;*

b) ***comunicare il nome e i dati di contatto del responsabile della protezione dei dati*** *o di altro punto di contatto presso cui ottenere più informazioni;*

c) ***descrivere le probabili conseguenze della violazione dei dati personali****;*

d) ***descrivere le misure adottate*** *o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.*

4. Qualora e nella misura in cui ***non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.***

5. Il titolare del trattamento ***documenta qualsiasi violazione dei dati personali****, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.*

- **notificare (se possibile entro 72 ore);**
- **informare;**
- **descrivere la natura, le probabili conseguenze e le misure adottate;**
- **documentare.**

Risarcimento e responsabilità

Articolo 82 GDPR

Diritto al risarcimento e responsabilità

1. Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.

2. Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.

3. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

4. Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.

5. Qualora un titolare del trattamento o un responsabile del trattamento abbia pagato, conformemente al paragrafo 4, l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno conformemente alle condizioni di cui al paragrafo 2.

6. Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79, paragrafo 2.

- **diritto al risarcimento;**
- **ATTENZIONE: inversione onere della prova!**
- **responsabilità solidale.**

Cosa fare?

... qualora non avessi fatto nulla.

STRATEGIA
definizione di un piano di intervento e le persone responsabili

VERIFICA ATTIVITA'
alla luce dei dati trattati

VERIFICA FLUSSO DEI DATI
flusso di dati all'interno e all'esterno dell'azienda

ESAME INFRASTRUTTURA
verifica che l'infrastruttura tecnica sia adeguata e conforme

VERIFICA E ADEGUAMENTO CONTRATTI
richiedere ai fornitori di servizio garanzie circa la conformità con il GDPR

FORMAZIONE PERSONALE
la corretta gestione dei dati presuppone un'adeguata e costante formazione dei collaboratori

REGOLE D'ORO

In caso di dubbio si consiglia di minimizzare i dati trattati, evitare di conservare dati inutili e di raccogliere solo le informazioni indispensabili.

Garantirsi sempre pieno controllo e accesso ai dati dei clienti presso terzi.

Punti del contratto (1/3)

elenco esemplificativo

oggetto e durata
descrivere nel dettaglio l'oggetto della prestazione (vedi art. 4 cpv. 2 e 28 GDPR)

modalità, scopo e categorie dei dati
descrivere le modalità del trattamento e la tipologia e la categoria dei dati (vedi art. 4 GDPR)

diritti e obblighi del titolare
compiti del titolare (vedi art. 6 cpv. 1, 12 ss GDPR), prevedere la forma scritta per le istruzioni

persone di contatto fra le parti
di modo che le istruzioni siano date e ricevute solo da persone autorizzate da ambo le parti

obblighi del responsabile
di fatto i punti elencati dall'art. 28 cpv. 3 GDPR

ATTENZIONE: questo elenco vuole fornire degli spunti pratici; si raccomanda di fare allestire/verificare il contratto da un legale o da un giurista.

Punti del contratto (2/3)

obbligo di notifica del responsabile
indicare quanto previsto agli artt. 33 e 34 GDPR

condizioni di subdelega
esclusione parziale o totale e/o obblighi ex art. art. 28 cpv. 3 seconda frase let. d GDPR

misure tecniche e organizzative (art. 32 GDPR)
specificare se sono date le condizioni e quali misure devono essere prese

obblighi del responsabile alla fine del contratto
vedi art. 28 cpv. 3 seconda frase let. g GDPR

condizioni di remunerazione
specificare il compenso per le prestazioni

ATTENZIONE: questo elenco vuole fornire degli spunti pratici; si raccomanda di fare allestire/verificare il contratto da un legale o da un giurista.

Punti del contratto (3/3)

responsabilità
vedi art. 82 GDPR

obbligo di conservazione documentazione
prevedere che il responsabile conservi la documentazione comprovante la sua attività

pena convenzionale
oltre al risarcimento danni, quale deterrente e garanzia

clausola di salvaguardia
a tutela della validità del contratto in caso di vizio parziale

forma (scritta), diritto applicabile e foro
ad esempio per quanto di carattere non imperativo foro CH e diritto sostanziale svizzero

ATTENZIONE: questo elenco vuole fornire degli spunti pratici; si raccomanda di fare allestire/verificare il contratto da un legale o da un giurista.

Domande?

Oggi è solo l'inizio. Il GDPR non può essere considerato un regolamento statico e, con la sua applicazione, vi saranno certamente sviluppi importanti. Occorre quindi aggiornarsi di continuo.

Grazie per l’attenzione!

avv. Rocco Talleri

rocco@talleri.ch

Talleri Law Studio legale

Crocicchio Cortogna 2
CP 6544
CH -6901 Lugano
www.talleri.law