UNIVERSITÀ POLITECNICA DELLE MARCHE

DII Dipartimento di Ingegneria dell'Informazione

unimc

Art. 32 Gdpr: disponibilità e resilienza. Diritti sul trattamento e diritto al trattamento.

Francesco Cucci

avvocato

LTS CONSULTING – LEGAL TECH SECURITY – Gruppo di lavoro - RIMINI

Tel 054156050 – cell 3713305150 email fcucci@studiolegalecucci.net

Martedì 19 Luglio 2022

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

OGGETTO DELL'ELABORATO

Con il presente elaborato si cercherà di verificare:

- La **distinzione** tra **disponibilità** e **resilienza** del trattamento
- Il fatto che **disponibilità** e **resilienza** **NON** siano valori assoluti.
- Quali siano le **minacce** alla **resilienza** e le **misure** per garantirla

Disponibilità e resilienza

Esaminiamo questi due concetti

Dove se ne parla?

Articolo 32

Sicurezza del trattamento

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 adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) …

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

Disponibilità e resilienza

Esaminiamo questi due concetti

Dove se ne parla?

Articolo 32

Sicurezza del trattamento

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 adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) …

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

Disponibilità e resilienza

Esaminiamo questi due concetti

Dove se ne parla?

Articolo 32

Sicurezza del trattamento

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 adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) …

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

Disponibilità e resilienza

Esaminiamo questi due concetti

Dove se ne parla?

Articolo 32

Sicurezza del trattamento

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 adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) ...

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

Disponibilità e resilienza

Esaminiamo questi due concetti

Dove se ne parla?

Articolo 32

Sicurezza del trattamento

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 adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) ...

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

Disponibilità e resilienza

Esaminiamo questi due concetti

Dove se ne parla?

Articolo 32

Sicurezza del trattamento

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 adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) ...

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

Disponibilità e resilienza

Esaminiamo questi due concetti

Dove se ne parla?

Articolo 32

Sicurezza del trattamento

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 adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) ...

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

Disponibilità e resilienza

Esaminiamo questi due concetti

Dove se ne parla?

Articolo 32

Sicurezza del trattamento

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 adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) …

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

Disponibilità e resilienza

Esaminiamo questi due concetti

Dove se ne parla?

Articolo 32

Sicurezza del trattamento

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 adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) …

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

riservatezza,

riservatezza, integrità

riservatezza, integrità e disponibilità

riservatezza, integrità e disponibilità

i cosiddetti parametri RID

sono le caratteristiche che l'art. 4, par. 1, n. 2 della Direttiva NIS, chiede di garantire, sia per i dati in sé, che per i servizi offerti o accessibili tramite rete, **al fine di assicurare la** «sicurezza della rete e dei sistemi informativi»,.

Dobbiamo quindi interrogarci su

Quale senso abbia

attribuire i parametri RID ai **sistemi** e ai

Servizi anziché ai dati personali in sé,

partendo dal presupposto che si tratti, ovviamente, di aspetti che il GDPR ha voluto tenere distinti.

RISERVATEZZA DI UN SISTEMA O DI UN SERVIZIO

riguarda **l'esistenza** in sé del sistema e del servizio, intesi come struttura (sistema) e "funzioni" che può erogare (servizi), in relazione al trattamento di dati personali.

Tradotto: necessità di nascondere e segregare il sistema in sé – ed i servizi da esso erogabili - rispetto a chi non è autorizzato a conoscerlo e ad accedervi.

INTEGRITA' DI UN SISTEMA O DI UN SERVIZIO

riguarda la **struttura** in sé del sistema e dei servizi erogabili, intesa come garanzia contro modifiche non volute al sistema o al servizio, sia per colpa: "errori"; che per dolo: "sabotaggi".

Tradotto: necessità di impedire che il sistema - ed i servizi da esso erogabili – subiscano modifiche non desiderabili.

DISPONIBILITA’ DI UN SISTEMA O DI UN SERVIZIO

riguarda la **fruibilità** in sé del sistema e del servizio, intesa come garanzia di potervi accedere e fruire dei servizi in un dato momento

Tradotto: necessità di garantire la continuità della funzionalità del sistema e dei servizi erogabili.

RESILIENZA DI UN SISTEMA O DI UN SERVIZIO

RESILIENZA

SIGNIFICATO DI UNA PAROLA ABUSATA:

resilienza [re-si-lièn-za] n.f.

1. (fis.) **proprietà dei materiali di resistere agli urti senza spezzarsi**, rappresentata dal rapporto tra il lavoro necessario per rompere una barretta di un materiale e la sezione della barretta stessa

2. **capacità di resistere e di reagire di fronte a difficoltà, avversità, eventi negativi** ecc.: resilienza sociale

(cfr. garzantilinguistica.it)

In ambito tecnico con *resiliens* si indica «la capacità di un corpo di **assorbire l'energia di un urto contraendosi,** oppure quella **di riassumere la forma originaria una volta sottoposto a una deformazione**" (L'elasticità di resilienza, accademiadellacrusca.it, 12/12/2014).

DEFINIZIONE PREFERIBILE

“capacità … di riassumere la forma originaria una volta sottoposto a una deformazione (attacco)”.

La qualità di “**resistere agli urti senza spezzarsi**” andrebbe infatti a coincidere e a **duplicare** le stesse qualità di “**disponibilità ed integrità**”:

se **dopo un urto/attacco** il **sistema** ed il **servizio** sono ancora **integri** e **disponibili**, significa che hanno resistito passivamente all’attacco/urto e **non si sono «spezzati».**

Nel GDPR la parola «**resilienza**» viene utilizzata una sola volta: solo qui, in questo paragrafo dell'art. 32 **!**

Differenze tra

“disponibilità ed integrità”

e

“resilienza”

Disponibilità ed Integrità sono

qualità statiche

che possiamo verificare in un dato momento.

Resilienza è una **qualità dinamica**.

Disponibilità ed Integrità del sistema e del servizio riguardano il momento in cui si fa la verifica e devono essere garantiti, tendenzialmente, quali valori in sé

Disponibilità ed Integrità del sistema e del servizio riguardano il momento in cui si fa la verifica e devono essere garantiti, tendenzialmente, quali valori in sé

Disponibilità ed **Integrità** del sistema e del servizio riguardano il momento in cui si fa la verifica e devono essere garantiti, tendenzialmente, quali valori in sé

Disponibilità ed **Integrità** del sistema e del servizio riguardano il momento in cui si fa la verifica e **devono essere garantiti**, tendenzialmente, quali valori in sé

Disponibilità ed **Integrità** del sistema e del servizio riguardano il momento in cui si fa la verifica e **devono essere garantiti**, tendenzialmente, **quali valori in sé**

Resilienza riguarda, invece, proprio il momento in cui disponibilità ed integrità sono perse e deve essere garantita non quale valore in sé ma quale strumento per recuperare Disponibilità ed Integrità.

Resilienza riguarda, invece, proprio il momento in cui **disponibilità** ed integrità sono perse e deve essere garantita non quale valore in sé ma quale strumento per recuperare Disponibilità ed Integrità.

Resilienza riguarda, invece, proprio il momento in cui **disponibilità** ed **integrità** sono perse e deve essere garantita non quale valore in sé ma quale strumento per recuperare Disponibilità ed Integrità.

Resilienza riguarda, invece, proprio il momento in cui **disponibilità** ed **integrità sono perse** e deve essere garantita non quale valore in sé ma quale strumento per recuperare Disponibilità ed Integrità.

Resilienza riguarda, invece, proprio il momento in cui **disponibilità** ed **integrità sono perse** e deve essere garantita non quale valore in sé ma quale **strumento per recuperare Disponibilità** ed **Integrità**.

il fatto che un sistema ed un servizio siano anche resilienti, conta poco se, nel momento della concreta verifica, non si ha né disponibilità né integrità.

RISERVATEZZA E RESILIENZA NON SI PARLANO

La Resilienza non può riguardare la **Riservatezza del sistema o del servizio**, in quanto non **potrà ripristinarla a posteriori, una volta violata.**

DISPONIBILITA’ E RESILIENZA: QUALITA’ RELATIVE

Nel trattare dati personali l’obbligo di garantire RISERVATEZZA e INTEGRITA’, fintanto che è in atto il trattamento, è un obbligo permanente cui corrisponde un diritto altrettanto permanente, qualunque ne sia la base giuridica.

DISPONIBILITA’ E RESILIENZA: QUALITA’ RELATIVE

Nel trattare dati personali l’obbligo di garantire **RISERVATEZZA** e INTEGRITA’, fintanto che è in atto il trattamento, è un obbligo permanente cui corrisponde un diritto altrettanto permanente, qualunque ne sia la base giuridica.

DISPONIBILITA’ E RESILIENZA: QUALITA’ RELATIVE

Nel trattare dati personali l’obbligo di garantire **RISERVATEZZA** e **INTEGRITA**’, fintanto che è in atto il trattamento, è un obbligo permanente cui corrisponde un diritto altrettanto permanente, qualunque ne sia la base giuridica.

DISPONIBILITA’ E RESILIENZA: QUALITA’ RELATIVE

Nel trattare dati personali l’obbligo di garantire **RISERVATEZZA** e **INTEGRITA**’, fintanto che è in atto il trattamento, è un **obbligo permanente** cui corrisponde un diritto altrettanto permanente, qualunque ne sia la base giuridica.

DISPONIBILITA’ E RESILIENZA: QUALITA’ RELATIVE

Nel trattare dati personali l’obbligo di garantire **RISERVATEZZA** e **INTEGRITA**’, fintanto che è in atto il trattamento, è un **obbligo permanente** cui corrisponde un diritto altrettanto permanente, **qualunque ne sia la base giuridica.**

Quanto alla DISPONIBILITA’ dei dati in un certo momento, invece, occorre considerare che MANCANZA DI DISPONIBILITA’, significa anche assenza di trattamento in quel dato momento.

Quanto alla **DISPONIBILITA**’ dei dati in un certo momento, invece, occorre considerare che MANCANZA DI DISPONIBILITA’, significa anche assenza di trattamento in quel dato momento.

Quanto alla **DISPONIBILITA**’ dei dati in un certo momento, invece, occorre considerare che **MANCANZA DI DISPONIBILITA**’, significa anche assenza di trattamento in quel dato momento.

Quanto alla **DISPONIBILITA**’ dei dati in un certo momento, invece, occorre considerare che **MANCANZA DI DISPONIBILITA**’, **significa** anche assenza di trattamento in quel dato momento.

Quanto alla **DISPONIBILITA**’ dei dati in un certo momento, invece, occorre considerare che **MANCANZA DI DISPONIBILITA**’, **significa** anche **assenza di trattamento** in quel dato momento.

E’ bene chiarire che se non si dispone più dei dati perché sono stati cancellati definitivamente, ci troviamo di fatto davanti alla cessazione del trattamento.

E’ bene chiarire che **se non si dispone più dei dati** perché sono stati cancellati definitivamente, ci troviamo di fatto davanti alla cessazione del trattamento.

E’ bene chiarire che **se non si dispone più dei dati** perché sono stati **cancellati definitivamente**, ci troviamo di fatto davanti alla cessazione del trattamento.

E’ bene chiarire che **se non si dispone più dei dati** perché sono stati **cancellati definitivamente**, ci troviamo di fatto davanti alla **cessazione del trattamento**.

E’ bene chiarire che **se non si dispone più dei dati** perché sono stati **cancellati definitivamente**, ci troviamo di fatto davanti alla **cessazione del trattamento**.

Se invece i dati, oltre che essere stati cancellati, sono stati prima anche esfiltrati, allora il problema non riguarda più la disponibilità, ma la riservatezza.

E’ bene chiarire che **se non si dispone più dei dati** perché sono stati **cancellati definitivamente**, ci troviamo di fatto davanti alla **cessazione del trattamento**.

Se invece i dati, oltre che essere stati cancellati, sono stati prima anche esfiltrati, allora il problema non riguarda più la disponibilità, ma la riservatezza.

E’ bene chiarire che **se non si dispone più dei dati** perché sono stati **cancellati definitivamente**, ci troviamo di fatto davanti alla **cessazione del trattamento**.

Se invece i dati, **oltre** che essere stati **cancellati**, sono stati prima anche esfiltrati, allora il problema non riguarda più la disponibilità, ma la riservatezza.

E’ bene chiarire che **se non si dispone più dei dati** perché sono stati **cancellati definitivamente**, ci troviamo di fatto davanti alla **cessazione del trattamento**.

Se invece i dati, **oltre** che essere stati **cancellati**, sono stati prima **anche esfiltrati**, allora il problema non riguarda più la disponibilità, ma la riservatezza.

E’ bene chiarire che **se non si dispone più dei dati** perché sono stati **cancellati definitivamente**, ci troviamo di fatto davanti alla **cessazione del trattamento**.

Se invece i dati, **oltre** che essere stati **cancellati**, sono stati prima **anche esfiltrati**, allora il **problema** non riguarda più la disponibilità, ma la riservatezza.

E’ bene chiarire che **se non si dispone più dei dati** perché sono stati **cancellati definitivamente**, ci troviamo di fatto davanti alla **cessazione del trattamento**.

Se invece i dati, **oltre** che essere stati **cancellati**, sono stati prima **anche esfiltrati**, allora il **problema** non riguarda più la disponibilità, ma la **riservatezza**.

E’ bene chiarire che **se non si dispone più dei dati** perché sono stati **cancellati definitivamente**, ci troviamo di fatto davanti alla **cessazione del trattamento**.

Se invece i dati, **oltre** che essere stati **cancellati**, sono stati prima **anche esfiltrati**, allora il **problema** non riguarda più la disponibilità, ma la **riservatezza**.

Esaminando la fattispecie della indisponibilità “secca” (cioè priva di ulteriori connotazioni che possano mettere in gioco altri parametri RID), si può concludere che se il dato è indisponibile non è più possibile trattarlo.

E’ bene chiarire che **se non si dispone più dei dati** perché sono stati **cancellati definitivamente**, ci troviamo di fatto davanti alla **cessazione del trattamento**.

Se invece i dati, **oltre** che essere stati **cancellati**, sono stati prima **anche esfiltrati**, allora il **problema** non riguarda più la disponibilità, ma la **riservatezza**.

Esaminando la fattispecie della **indisponibilità “secca”** (cioè priva di ulteriori connotazioni che possano mettere in gioco altri parametri RID), si può concludere che se il dato è indisponibile non è più possibile trattarlo.

E’ bene chiarire che **se non si dispone più dei dati** perché sono stati **cancellati definitivamente**, ci troviamo di fatto davanti alla **cessazione del trattamento**.

Se invece i dati, **oltre** che essere stati **cancellati**, sono stati prima **anche esfiltrati**, allora il **problema** non riguarda più la disponibilità, ma la **riservatezza**.

Esaminando la fattispecie della **indisponibilità “secca”** (cioè priva di ulteriori connotazioni che possano mettere in gioco altri parametri RID), si può concludere che **se il dato è indisponibile** non è più possibile trattarlo.

E’ bene chiarire che **se non si dispone più dei dati** perché sono stati **cancellati definitivamente**, ci troviamo di fatto davanti alla **cessazione del trattamento**.

Se invece i dati, **oltre** che essere stati **cancellati**, sono stati prima **anche esfiltrati**, allora il **problema** non riguarda più la disponibilità, ma la **riservatezza**.

Esaminando la fattispecie della **indisponibilità “secca”** (cioè priva di ulteriori connotazioni che possano mettere in gioco altri parametri RID), si può concludere che **se il dato è indisponibile non è più possibile trattarlo**.

Se non è più possibile effettuare alcun trattamento, cade anche il diritto dell’interessato a pretendere il rispetto dei parametri RID, proprio perché non esiste più alcun trattamento di dati personali che a tali parametri debba conformarsi.

Se non è più possibile effettuare alcun trattamento, cade anche il diritto dell'interessato a pretendere il rispetto dei parametri RID, proprio perché non esiste più alcun trattamento di dati personali che a tali parametri debba conformarsi.

Se non è più possibile effettuare alcun trattamento, cade anche il diritto dell'interessato a pretendere il rispetto dei parametri RID, proprio perché **non esiste più alcun trattamento** di dati personali che a tali parametri debba conformarsi.

Se non è più possibile effettuare alcun trattamento, cade anche il diritto dell'interessato a pretendere il rispetto dei parametri RID, proprio perché **non esiste più alcun trattamento** di dati personali che a tali parametri debba conformarsi.

Ci dobbiamo chiedere, dunque, quando permanga in capo all'interessato il diritto di pretendere la disponibilità del dato (e, conseguentemente, anche la disponibilità e resilienza dei sistemi e dei servizi di trattamento).

Se non è più possibile effettuare alcun trattamento, cade anche il diritto dell'interessato a pretendere il rispetto dei parametri RID, proprio perché **non esiste più alcun trattamento** di dati personali che a tali parametri debba conformarsi.

Ci dobbiamo chiedere, dunque, **quando** permanga in capo all'interessato il diritto di pretendere la disponibilità del dato (e, conseguentemente, anche la disponibilità e resilienza dei sistemi e dei servizi di trattamento).

Se non è più possibile effettuare alcun trattamento, cade anche il diritto dell'interessato a pretendere il rispetto dei parametri RID, proprio perché **non esiste più alcun trattamento** di dati personali che a tali parametri debba conformarsi.

Ci dobbiamo chiedere, dunque, **quando** permanga in capo all'interessato il **diritto di pretendere la disponibilità del dato** (e, conseguentemente, anche la disponibilità e resilienza dei sistemi e dei servizi di trattamento).

Se non è più possibile effettuare alcun trattamento, cade anche il diritto dell'interessato a pretendere il rispetto dei parametri RID, proprio perché **non esiste più alcun trattamento** di dati personali che a tali parametri debba conformarsi.

Ci dobbiamo chiedere, dunque, **quando** permanga in capo all'interessato il **diritto di pretendere la disponibilità del dato** (e, conseguentemente, anche la **disponibilità** e resilienza dei sistemi e dei servizi di trattamento).

Se non è più possibile effettuare alcun trattamento, cade anche il diritto dell'interessato a pretendere il rispetto dei parametri RID, proprio perché **non esiste più alcun trattamento** di dati personali che a tali parametri debba conformarsi.

Ci dobbiamo chiedere, dunque, **quando** permanga in capo all'interessato il **diritto di pretendere la disponibilità del dato** (e, conseguentemente, anche la **disponibilità** e **resilienza** dei sistemi e dei servizi di trattamento).

Se non è più possibile effettuare alcun trattamento, cade anche il diritto dell'interessato a pretendere il rispetto dei parametri RID, proprio perché **non esiste più alcun trattamento** di dati personali che a tali parametri debba conformarsi.

Ci dobbiamo chiedere, dunque, **quando** permanga in capo all'interessato il **diritto di pretendere la disponibilità del dato** (e, conseguentemente, anche la **disponibilità** e **resilienza** dei **sistemi e dei servizi di trattamento**).

Ci dobbiamo interrogare, quindi, NON in ordine ai diritti dell’interessato SUL trattamento, ma in ordine ai diritti dell’interessato AL trattamento.

Ci dobbiamo interrogare, quindi, **NON** in ordine ai diritti dell'interessato SUL trattamento, ma in ordine ai diritti dell'interessato AL trattamento.

Ci dobbiamo interrogare, quindi, **NON** in ordine ai diritti dell'interessato **SUL** trattamento, ma in ordine ai diritti dell'interessato AL trattamento.

Ci dobbiamo interrogare, quindi, **NON** in ordine ai diritti dell'interessato **SUL** trattamento, ma in ordine ai diritti dell'interessato **AL** trattamento.

? Quando sorge il diritto **AL** trattamento, il diritto, cioè, **a che il trattamento continui a favore dell'interessato**, indipendentemente o anche contro la volontà del Titolare?

BASI GIURIDICHE DEL TRATTAMENTO

Conosciamo tutti le basi giuridiche del trattamento dei dati personali:

a) l'interessato ha espresso il **consenso** al trattamento dei propri dati personali per una o più specifiche finalità;

b) il trattamento è necessario all'esecuzione di un **contratto** di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) il trattamento è necessario per adempiere un **obbligo legale** al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per la salvaguardia degli **interessi vitali** dell'interessato o di un'altra persona fisica;

e) il trattamento è necessario per l'esecuzione di un **compito di interesse pubblico** o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

f) il trattamento è necessario per il perseguimento del **legittimo interesse** del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

APPARENTEMENTE, TUTTE LE BASI GIURIDICHE HANNO IN SÉ L'OBBLIGO DI GARANTIRE LA DISPONIBILITA' DEL DATO E QUINDI LA DISPONIBILITA' E LA RESILIENZA DEI SISTEMI E DEI SERVIZI DI TRATTAMENTO

ECCETTO...

BASI GIURIDICHE DEL TRATTAMENTO

a) l'interessato ha espresso il **consenso** al trattamento dei propri dati personali per una o più specifiche finalità;

b) il trattamento è necessario all'esecuzione di un **contratto** di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) il trattamento è necessario per adempiere un **obbligo legale** al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per la salvaguardia degli **interessi vitali** dell'interessato o di un'altra persona fisica;

e) il trattamento è necessario per l'esecuzione di un **compito di interesse pubblico** o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

f) il trattamento è necessario per il perseguimento del **legittimo interesse** del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

BASI GIURIDICHE DEL TRATTAMENTO

No disponibilità e resilienza

a) l'interessato ha espresso il **consenso** al trattamento dei propri dati personali per una o più specifiche finalità;

b) il trattamento è necessario all'esecuzione di un **contratto** di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) il trattamento è necessario per adempiere un **obbligo legale** al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per la salvaguardia degli **interessi vitali** dell'interessato o di un'altra persona fisica;

e) il trattamento è necessario per l'esecuzione di un **compito di interesse pubblico** o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

f) il trattamento è necessario per il perseguimento del **legittimo interesse** del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

BASI GIURIDICHE DEL TRATTAMENTO

No disponibilità e resilienza

a) l'interessato ha espresso il **consenso** al trattamento dei propri dati personali per una o più specifiche finalità;

b) il trattamento è necessario all'esecuzione di un **contratto** di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) il trattamento è necessario per adempiere un **obbligo legale** al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per la salvaguardia degli **interessi vitali** dell'interessato o di un'altra persona fisica;

e) il trattamento è necessario per l'esecuzione di un **compito di interesse pubblico** o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

f) il trattamento è necessario per il perseguimento del **legittimo interesse** del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

BASI GIURIDICHE DEL TRATTAMENTO

No disponibilità e resilienza

a) l'interessato ha espresso il **consenso** al trattamento dei propri dati personali per una o più specifiche finalità;

b) il trattamento è necessario all'esecuzione di un **contratto** di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

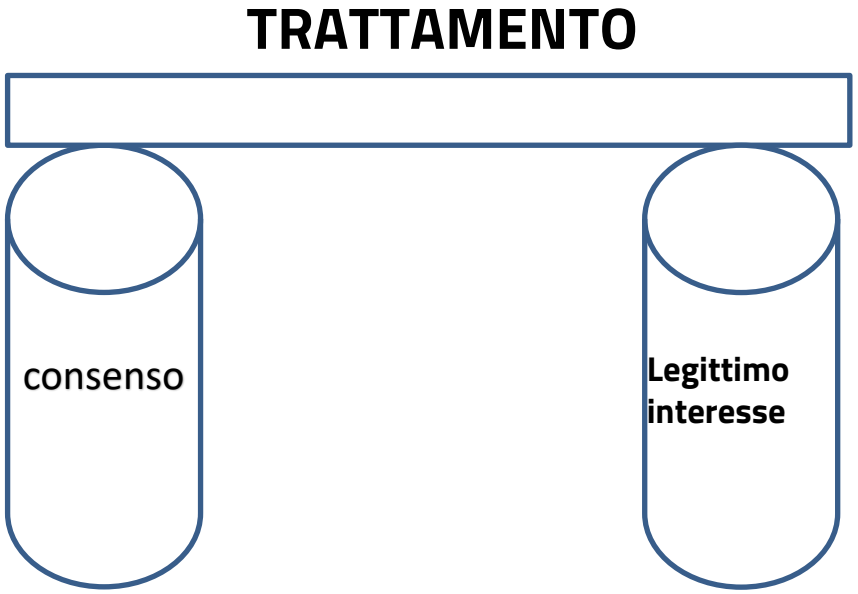
c) il trattamento è necessario per adempiere un **obbligo legale** al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per la salvaguardia degli **interessi vitali** dell'interessato o di un'altra persona fisica;

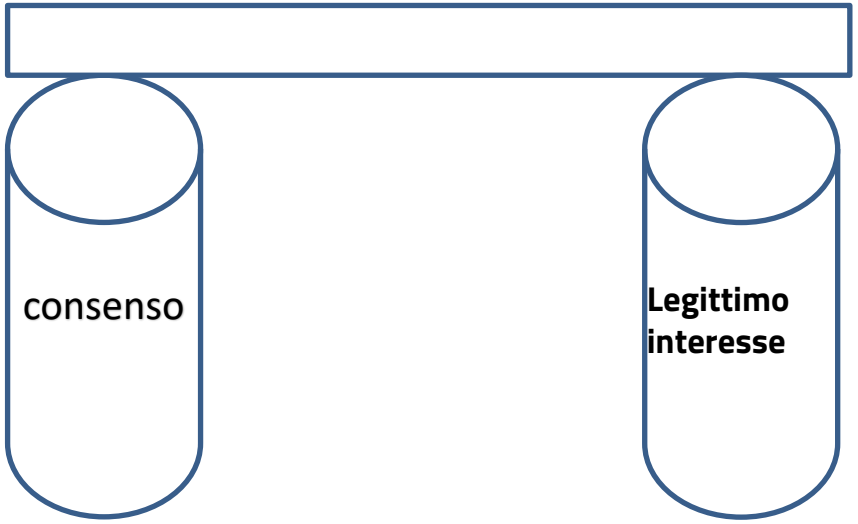
e) il trattamento è necessario per l'esecuzione di un **compito di interesse pubblico** o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

f) il trattamento è necessario per il perseguimento del **legittimo interesse** del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

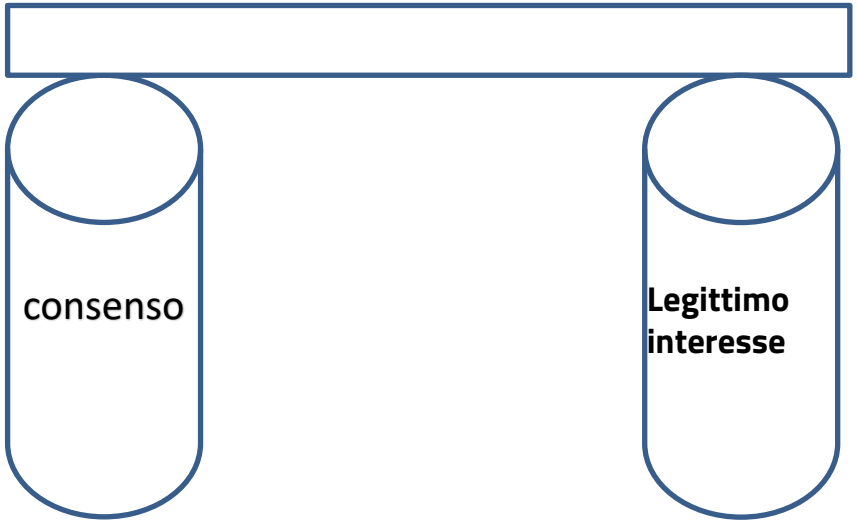
No disponibilità e resilienza



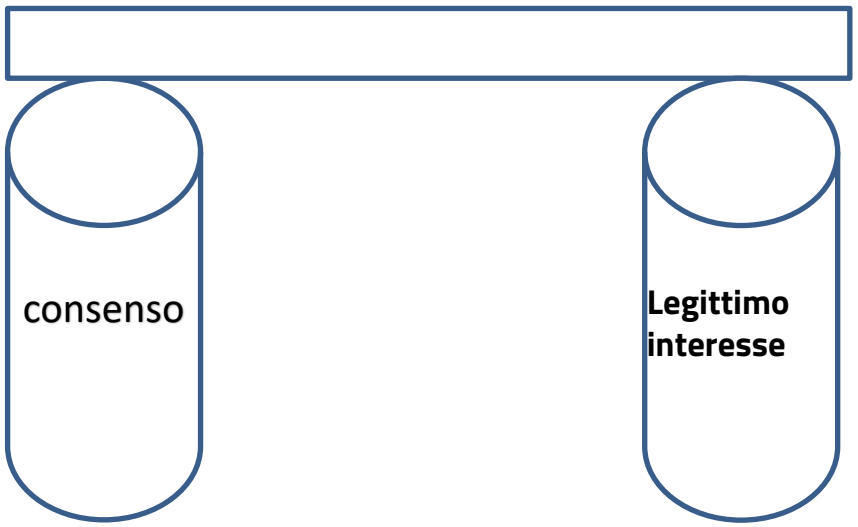
finché verrà svolto, l'interessato avrà diritto al rispetto dei requisiti di Riservatezza ed Integrità



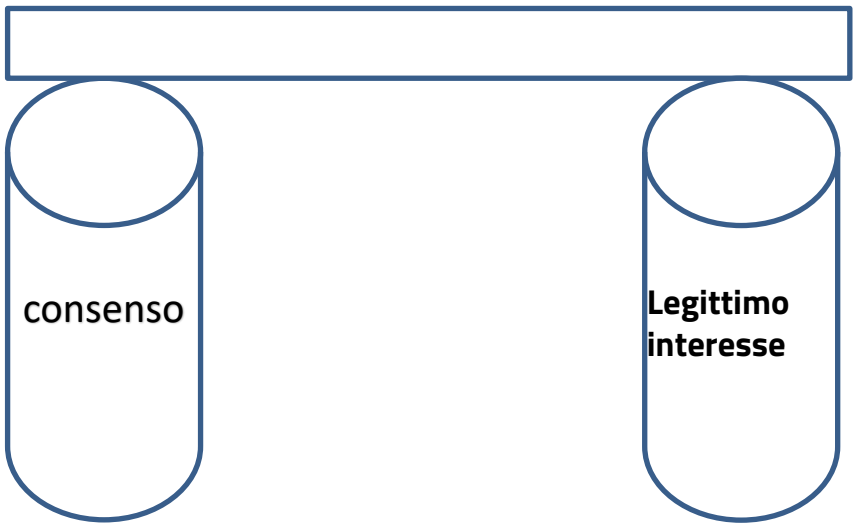
finché verrà svolto, l'interessato avrà diritto al rispetto dei requisiti di Riservatezza ed Integrità



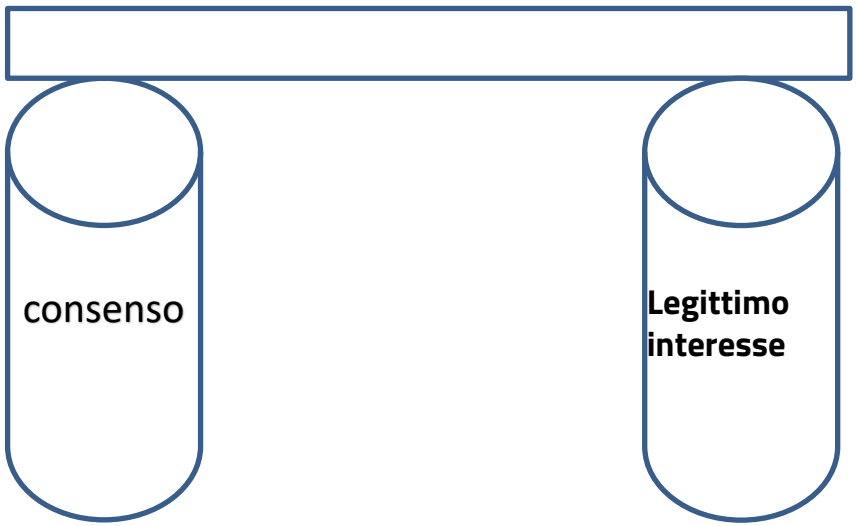
finché verrà svolto, **l'interessato** avrà diritto al rispetto dei requisiti di Riservatezza ed Integrità



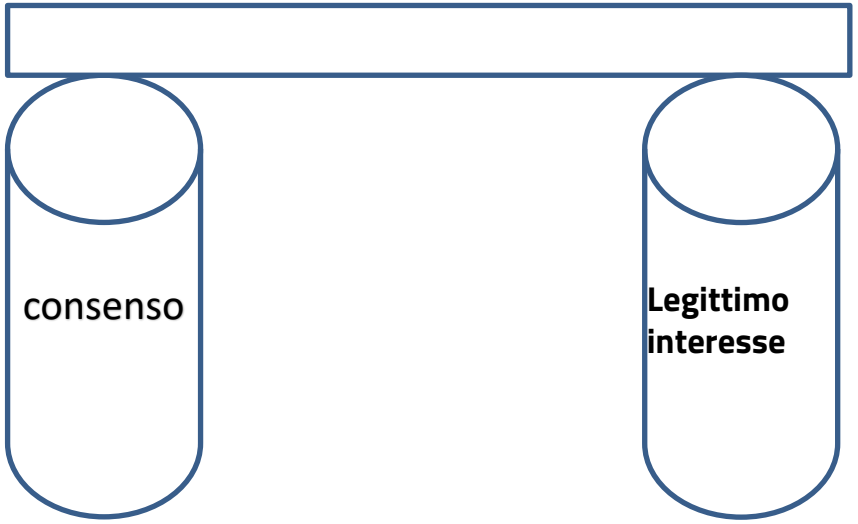
finché verrà svolto, **l'interessato** avrà **diritto** al rispetto dei requisiti di Riservatezza ed Integrità



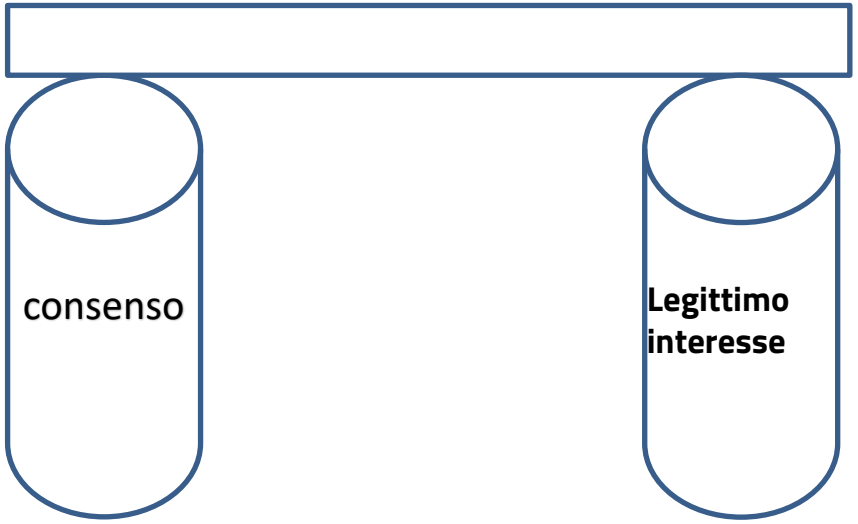
finché verrà svolto, **l'interessato** avrà **diritto** al rispetto dei requisiti di Riservatezza ed Integrità



finché verrà svolto, **l'interessato** avrà **diritto** al rispetto dei **requisiti** di Riservatezza ed Integrità

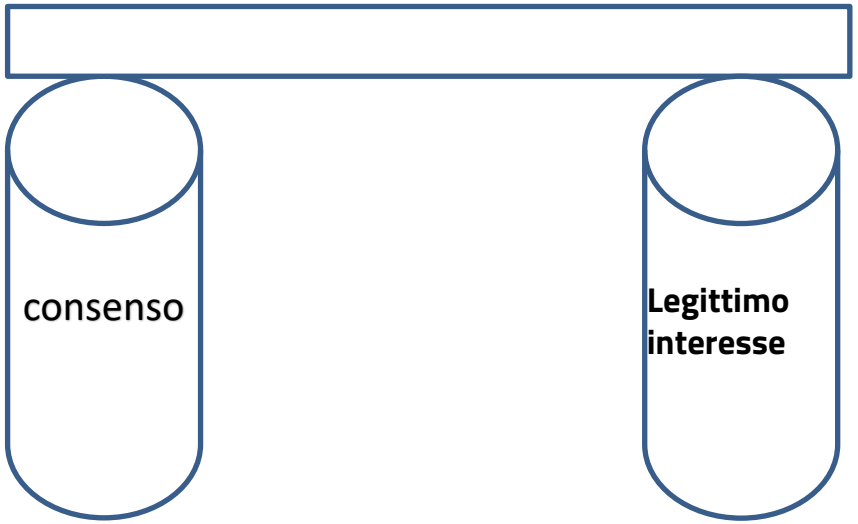


finché verrà svolto, **l'interessato** avrà **diritto** al rispetto dei **requisiti** di **Riservatezza** ed Integrità



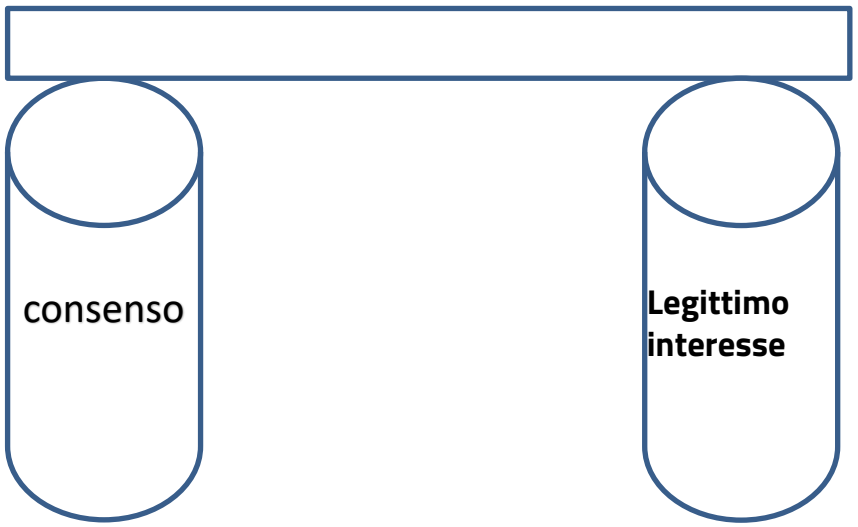
finché verrà svolto, **l'interessato** avrà **diritto** al rispetto dei **requisiti** di **Riservatezza** ed **Integrità**

TRATTAMENTO



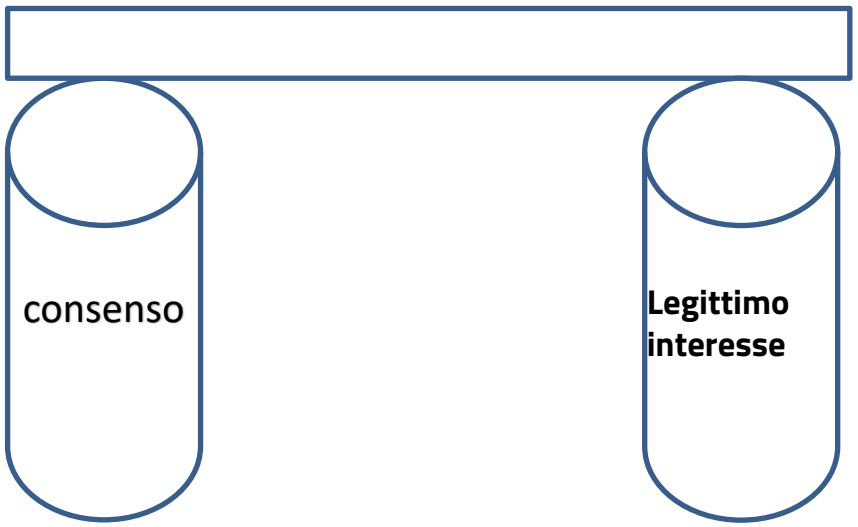
finché verrà svolto, **l'interessato** avrà **diritto** al rispetto dei **requisiti** di **Riservatezza** ed **Integrità**

NO diritto alla Disponibilità del dato e del trattamento, perché questo poggia, in entrambi i casi, sull'interesse esclusivo del titolare, che, quindi, ben può decidere di cessarlo.



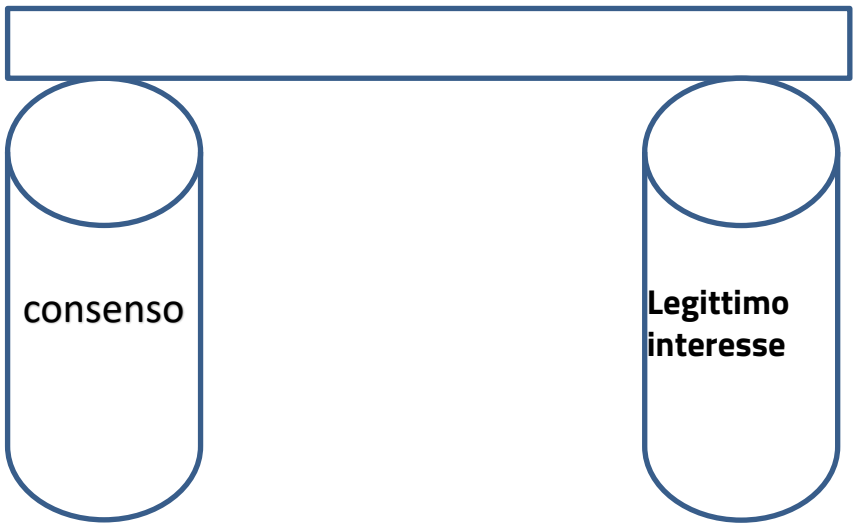
finché verrà svolto, **l'interessato** avrà **diritto** al rispetto dei **requisiti** di **Riservatezza** ed **Integrità**

NO ~~diritto alla Disponibilità~~ del dato e del trattamento, perché questo poggia, in entrambi i casi, sull'interesse esclusivo del titolare, che, quindi, ben può decidere di cessarlo.



finché verrà svolto, **l'interessato** avrà **diritto** al rispetto dei **requisiti** di **Riservatezza** ed **Integrità**

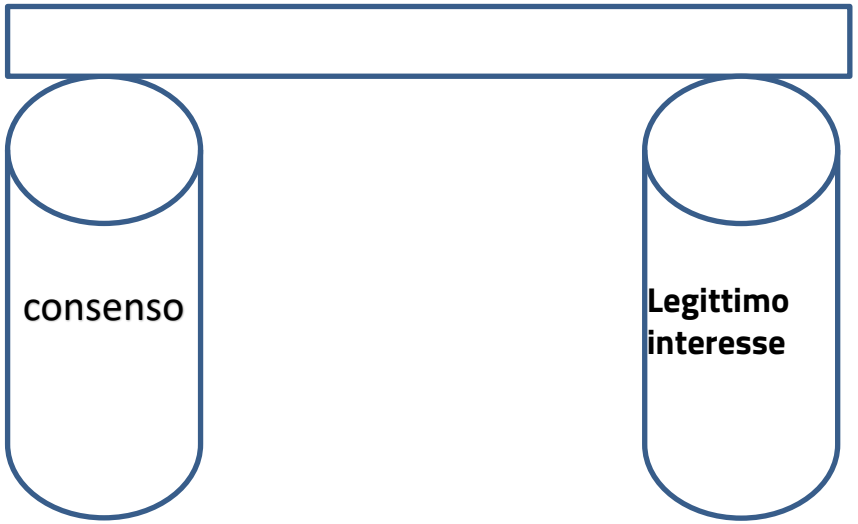
NO ~~diritto alla Disponibilità~~ del dato e del trattamento, perché questo poggia, in entrambi i casi, sull'interesse esclusivo del titolare, che, quindi, ben può decidere di cessarlo.



finché verrà svolto, **l'interessato** avrà **diritto** al rispetto dei **requisiti** di **Riservatezza** ed **Integrità**

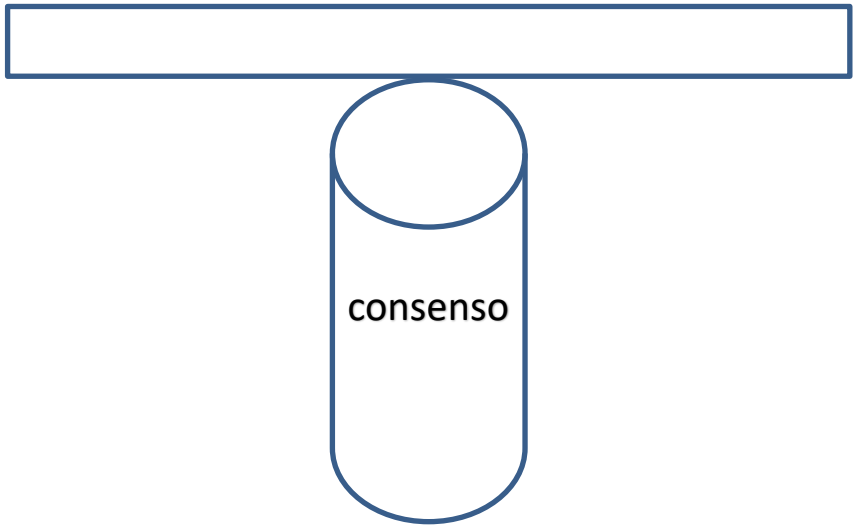
NO ~~diritto alla Disponibilità~~ del dato e del trattamento, perché questo poggia, in entrambi i casi, **sull'interesse esclusivo del titolare**, che, quindi, ben può decidere di cessarlo.

TRATTAMENTO

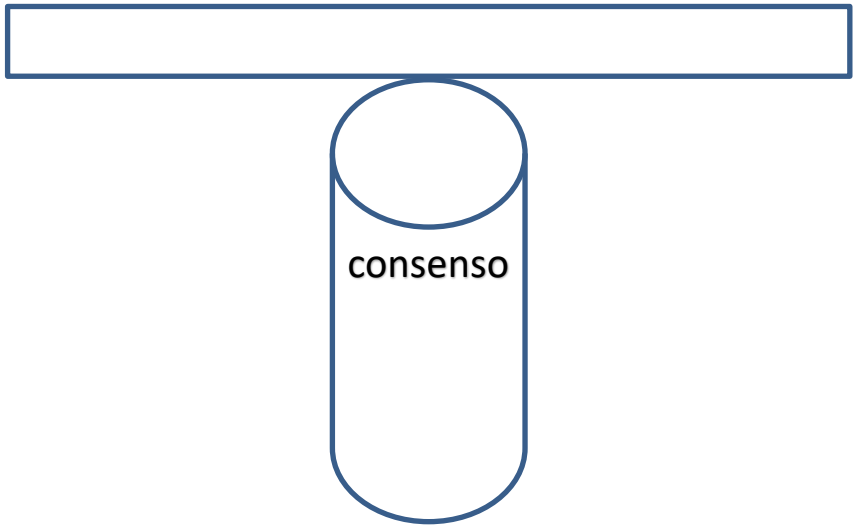


TRATTAMENTO

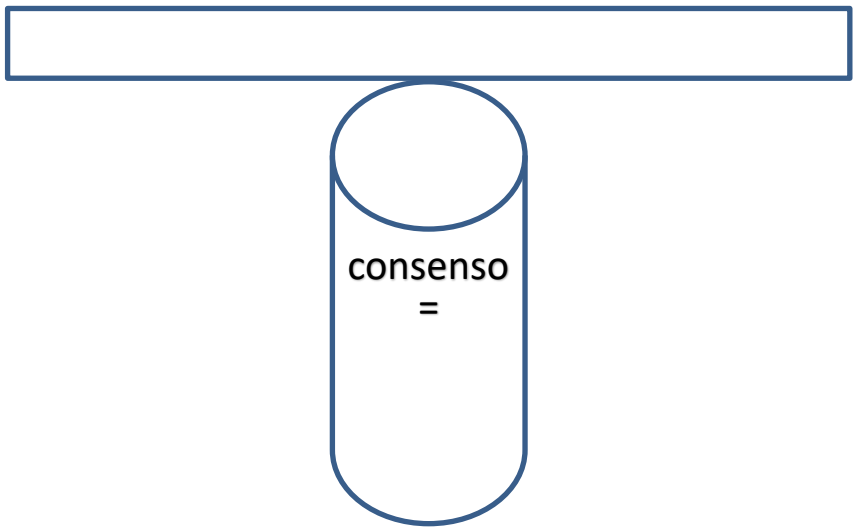
TRATTAMENTO



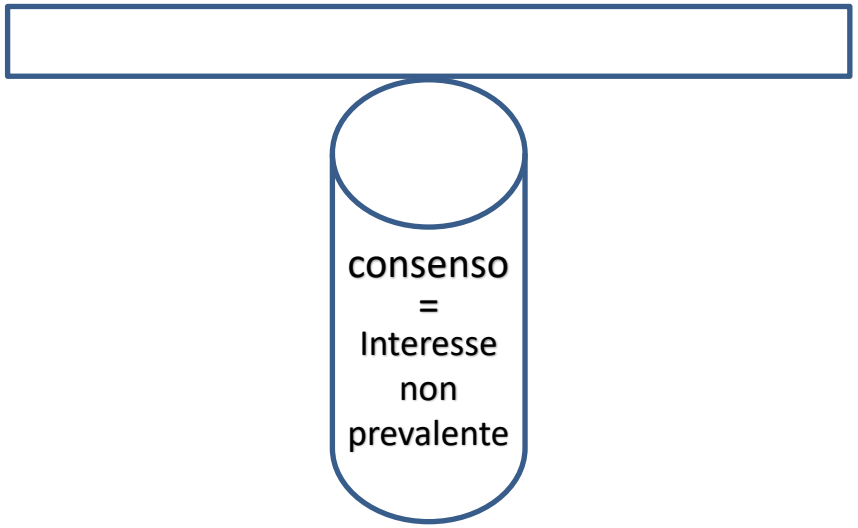
TRATTAMENTO



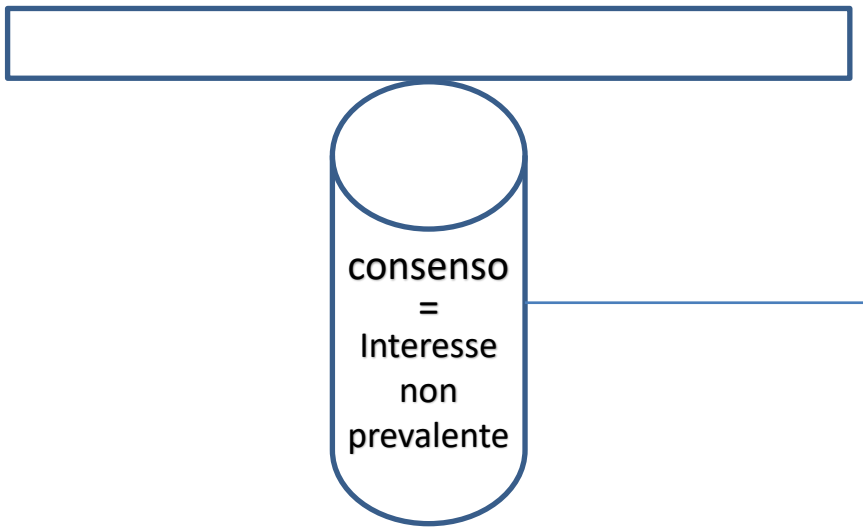
TRATTAMENTO



TRATTAMENTO



TRATTAMENTO



L'interesse del titolare non ha le caratteristiche di **prevalenza** sugli **interessi** o sui **diritti** e sulle **libertà dell'interessato**, **sicché**, per procedere al trattamento, **occorre** che il **Titolare raccolga** il **consenso** dell'interessato.

Quando il trattamento si fondi su una qualunque delle altre basi giuridiche, l'interessato, oltre a tutti i **diritti SUL** trattamento, vanta anche un **diritto AL trattamento**, cioè vanta il diritto che **l'attività** di **trattamento prosegua** e sia garantita nel momento in cui l'interessato stesso esercita i propri diritti.

Questo è **vero nell'ambito temporale** di **attuazione** della **finalità** su cui il trattamento poggia (il che è a dire: **all'interno del periodo di data retention obbligatoria**)

MINACCE ALLA **RESILIENZA** DEI **SISTEMI** E DEI **SERVIZI** DEL **TRATTAMENTO**

Cosa impedisce ad un sistema che ha subito un attacco/urto di “riprendere la propria forma”?

eccessiva rigidità

Il sistema tende a spezzarsi più che a piegarsi

eccessiva malleabilità

Il sistema, una volta piegato, non tende naturalmente a raddrizzarsi

eccessiva rigidità

Il sistema tende a spezzarsi più che a piegarsi

eccessiva malleabilità

Il sistema, una volta piegato, tende naturalme a raddrizzarsi

Fuor di metafora: tutto ciò che impedisce ad un sistema attaccato di tornare al punto immediatamente precedente l'attacco/urto sono le seguenti caratteristiche:

- la mancanza di memoria (com'ero ESATTAMENTE prima dell'attacco?)

- La mancanza di velocità (mi ricordo com'ero prima dell'attacco ma impiego un tempo intollerabilmente lungo per tornare a quel punto)

La gomma piuma, rispetto, ad esempio, alla memory foam, ha entrambe le qualità:

- Una volta compressa e decompressa ritorna esattamente com’era prima (memoria): qualità presente anche nella memory foam
- E ciò in tempi rapidissimi (velocità): qualità assente nella memory foam

Un sistema (o un servizio) si comporterà come la gomma piuma se:

- Avrà esatta memoria di com’era prima dell’attacco/urto
- Potrà ritornare a quello stato nei tempi più rapidi possibili

Viste le caratteristiche della «resilienza» dei sistemi e dei servizi, richiesta dal par. 1, lett. b dell'art. 32 del GDPR una domanda sorge spontanea:

Che differenza c'è tra resilienza dei sistemi e dei servizi e quanto richiesto alla lettera c) del medesimo paragrafo dell'art. 32 ???

Articolo 32

Sicurezza del trattamento

1. Omissis …

2. a)…
   b)…
   c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

Viste le caratteristiche della «resilienza» dei sistemi e dei servizi, richiesta dal par. 1, lett. b dell'art. 32 del GDPR una domanda sorge spontanea:

Che differenza c'è tra resilienza dei sistemi e dei servizi e quanto richiesto alla lettera c) del medesimo paragrafo dell'art. 32 ???

Articolo 32

Sicurezza del trattamento

1. Omissis …

2. a)…

   b)…

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

MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE PER GARANTIRE LA **RESILIENZA**

. Backup dei “DATI” con il minor RPO (Recovery Point Objective)

. Backup delle “CONFIGURAZIONI” di sistema (configurazioni di rete, configurazioni dei sistemi operativi, configurazione degli applicativi, ecc.) e DISASTER RECOVERY PLAN con il minor RTO (Recovery Time Objective)

. Backup della “CONNETTIVITÀ” WAN e LAN (ridondanza di provider e di router e firewall; ridondanza di switch o apparati di rete)

. Ridondanza (mirrored architecture): replica, no punto-punto, ma differita

. Soluzioni di verifica di integrità del dato replicato

. Replica di sistemi di Iperconvergenza (hyperconverged infrastracture)

. Procedure automatizzate di ripristino dei sistemi

. Procedure operative di ripristino

. Simulazioni ed esercitazioni di attuazione delle procedure operative

Francesco Cucci

Ancona, 19 luglio 2022