Epicentro italia srl
Via Aldo Moro, 48
25124 Brescia

Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali (prima parte)

14 APRILE 2018

CONSIGLIO NAZIONALE DELLA F.N.O.V.I

INTRODUZIONE

Il Regolamento Generale in materia di tutela dei dati personali, si propone di dare regole comuni a tutti gli Stati membri per la gestione e protezione dei dati personali.

Entro il 25 maggio 2018 il Parlamento/Governo e il Garante della privacy sono chiamati a compiere una complessa opera di **ADEGUAMENTO (dove necessario)** della normativa italiana al regolamento

INTRODUZIONE

UNA NUOVA NORMATIVA: PERCHE'?

RISOLVERE ALCUNI PROBLEMI

- ✓ APPLICAZIONE FRAMMENTATA DELLA NORMATIVA EUROPEA NEI VARI STATI MEMBRI
- ✓ INCERTEZZA GIURIDICA SULLE TUTELE
- ✓ NECESSITA' DI PROTEZIONE PIU' FORTE PER LE OPERAZIONI ONLINE ALLA LUCE DEL PROGRESSO TECNOLOGICO

GARANTIRE

- ✓ FAVORIRE LE ATTIVITA' ECONOMICHE E RENDERE PIU' TRASPARENTE LA CONCORRENZA.
- ✓ PERMETTE AGLI STATI DI ADEMPIERE AI PROPRI OBBLIGHI DI PROTEZIONE DEI CITTADINI (VITA PRIVATA E DATI)

OBIETTIVO MEDIATO

EFFETTIVA ED UNIFORME PROTEZIONE DEI DATI E LIBERA CIRCOLAZIONE DEI DATI

CHI È IL BENEFICIARIO DE TO?

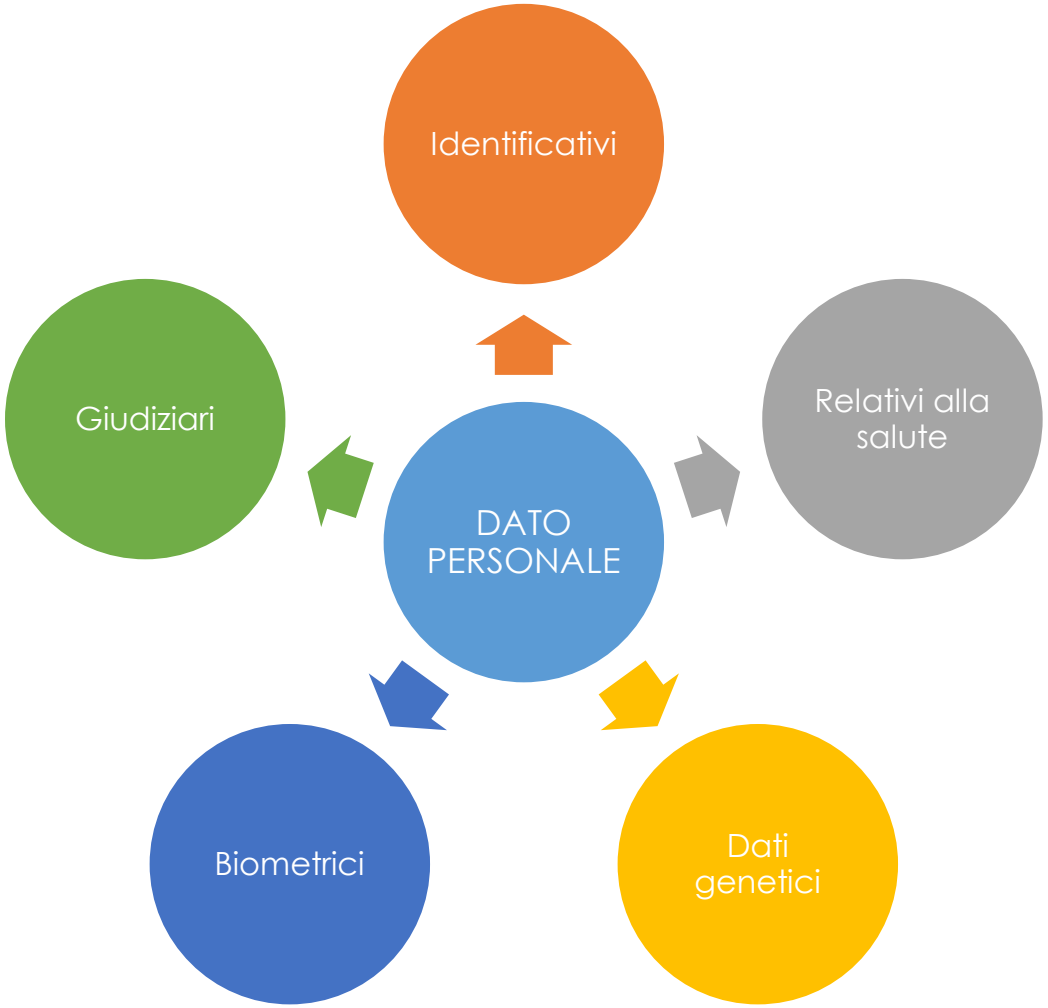
Il beneficiario del diritto alla protezione dei **DATI PERSONALI** è il soggetto **INTERESSATO** al **TRATTAMENTO** del **DATI PERSONALI**

QUAL E' IL SIGNIFICATO DI QUESTI TERMINI?

LE PAROLE CHIAVE

- DATO PERSONALE
- INTERESSATO
- TRATTAMENTO

Definizione di « dato personale »

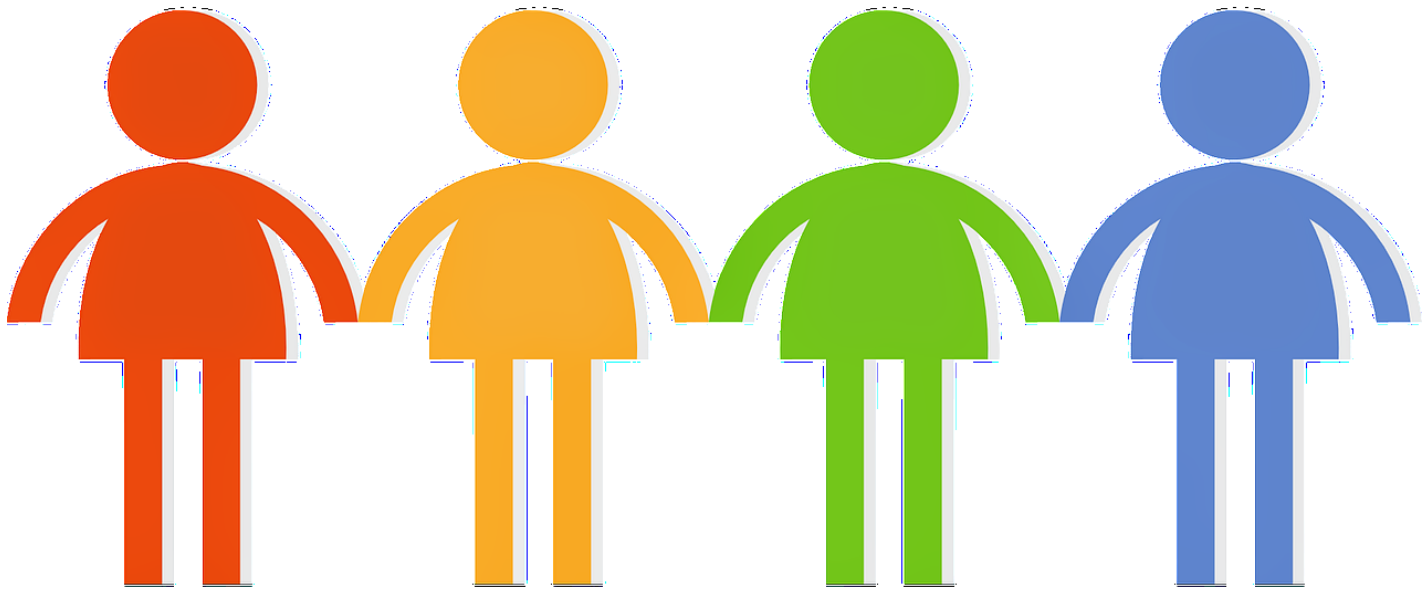


Altri dati oggetto di particolare tutela sono:

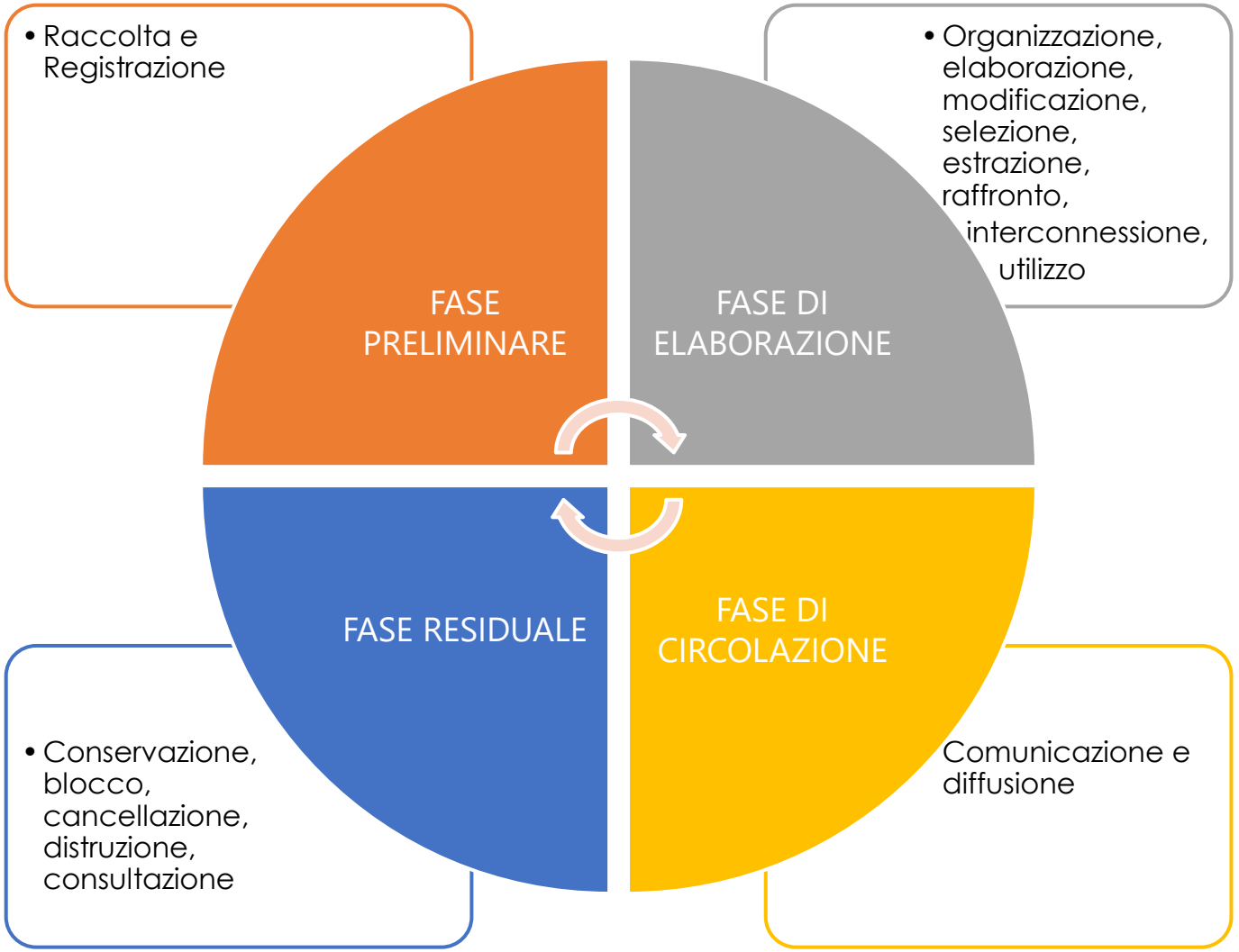
- Quelli relativi alle comunicazioni elettroniche (*uso di Internet o del telefono cellulare*)
- Quelli che consento la geolocalizzazione, fornendo informazioni sui luoghi frequentati e sugli spostamenti.

Definizione di « interessato»

E’ la persona fisica cui si riferiscono i dati personali, che è appunto oggetto della tutela del Regolamento.



Definizione di « trattamento»



Fonte: «Privacy. Protezione e tratatmento dei dati. Wolters Kluwer ItaiaSrl. Ed.2016

A CHI È DESTINATA LA NORMA?

Chi comunemente è soggetto alla normativa della privacy?

* Pubblica Amministrazione
* Banche
* Ospedali
* Associazioni
* Professionisti *(Medici, Avvocati, Commercialisti,…)*
* Aziende
* Siti Web
* …

Chi è ESCLUSO dalla normativa della privacy?

* IL REGOLAMENTO NON SI APPLICA AL TRATTAMENTO DI DATI PERSONALI EFFETTUATO DA UNA PERSONA FISICA NELL'AMBITO DI ATTIVITA' SENZA CONNESSIONE CON UN'ATTIVITÀ COMMERCIALE O PROFESSIONALE (Considerando n.18)

QUALI NOVITA' INTRODUCE IL NUOVO REGOLAMENTO EUROPEO?

SCOMPARE:

- ✓ **L'OBBLIGO DI NOTIFICAZIONE E DI VERIFICA PRELIMINARE AL GARANTE**
- ✓ **L'OBBLIGO DI RACCOLTA DEL CONSENSO IN FORMA SCRITTA**
- ✓ **IL DIRITTO DI BLOCCO COSI' COME E' STATO APPLICATO FINORA.**
- ✓ **LA DISTINZIONE TRA MISURE MINIME E IDONEE**

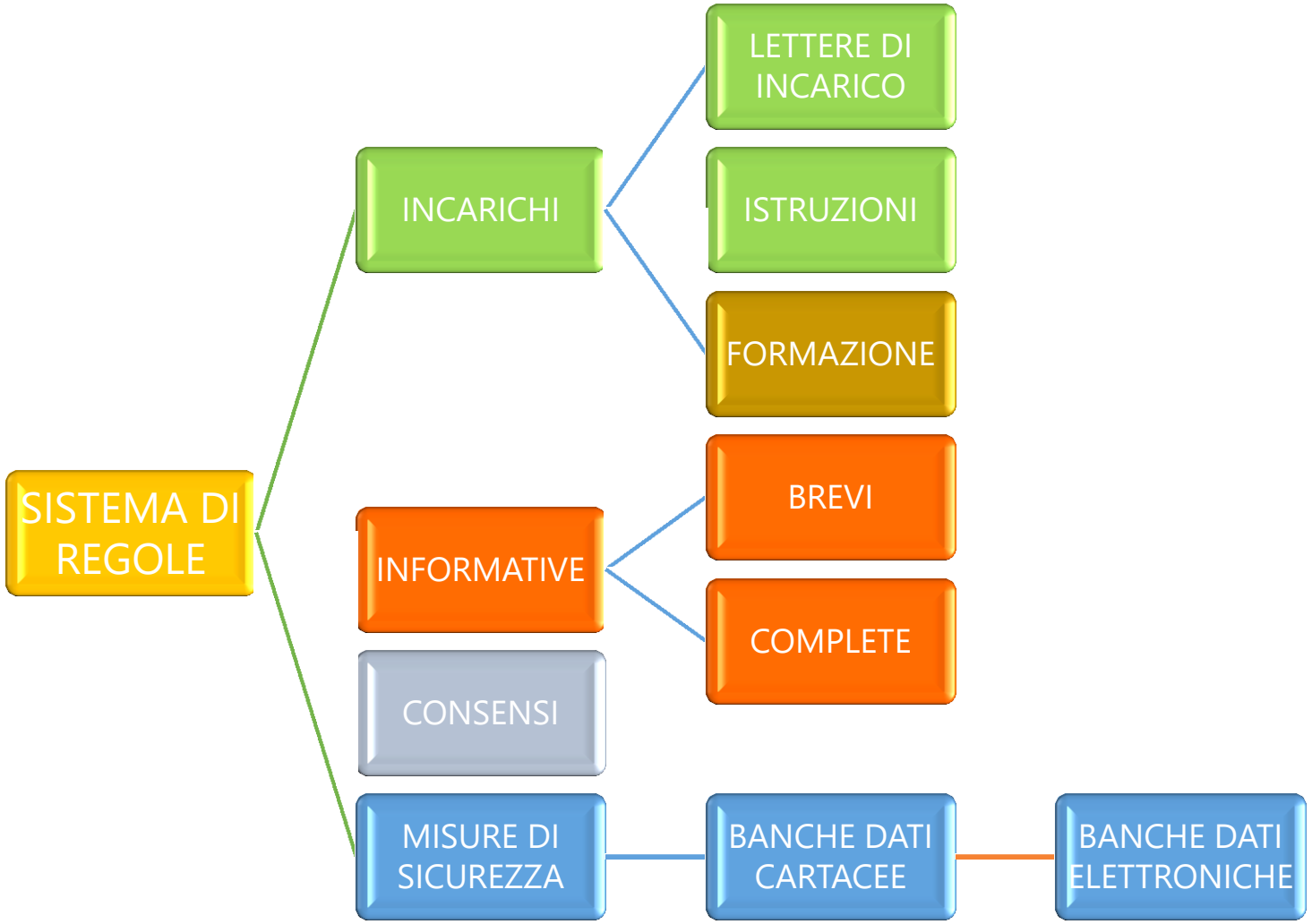
QUALI NOVITA' INTRODUCE IL NUOVO REGOLAMENTO EUROPEO?

MISURE ORGANIZZATIVE	MISURE TECNICHE INFORMATICHE
Introduzione del PRIVACY OFFICER	Adeguamento del sistema informativo per l'esercizio dei nuovi diritti: LIMITAZIONE, PORTABILITA' e OBLIO
Regolamentazione tramite atto giuridico del rapporto tra titolare e Responsabile esterno del trattamento o Co-Titolari del Trattamento dei dati personali	PSEUDONIMIZZAZIONE e CIFRATURA per la custodia e la trasmissione dei dati
Tenuta di un REGISTRO DEI TRATTAMENTI	Adeguamento tecnico per garantire RISERVATEZZA, INTEGRITA', DISPONIBILITA' e RESILIENZA del sistema informativo ai principi del nuovo regolamento
Adeguamento delle INFORMATIVE cartacee ed elettroniche	
Misure Organizzative volte a minimizzare i rischi rilevati, in quelli previsti nella VALUTAZIONE D'IMPATTO PER I TRATTAMENTI AD ALTO RISCHIO	Adeguamento tecnico per il RIPRISTINO TEMPESTIVO della disponibilità e l'accesso dei dati
PROCEDURE per l'esercizio dei NUOVI DIRITTI degli interessati: diritto di limitazione, portabilità e oblio; **Procedure di notifica al Garante di violazioni al sistema**	Misure per la tempestiva identificazione e gestione di violazioni al sistema

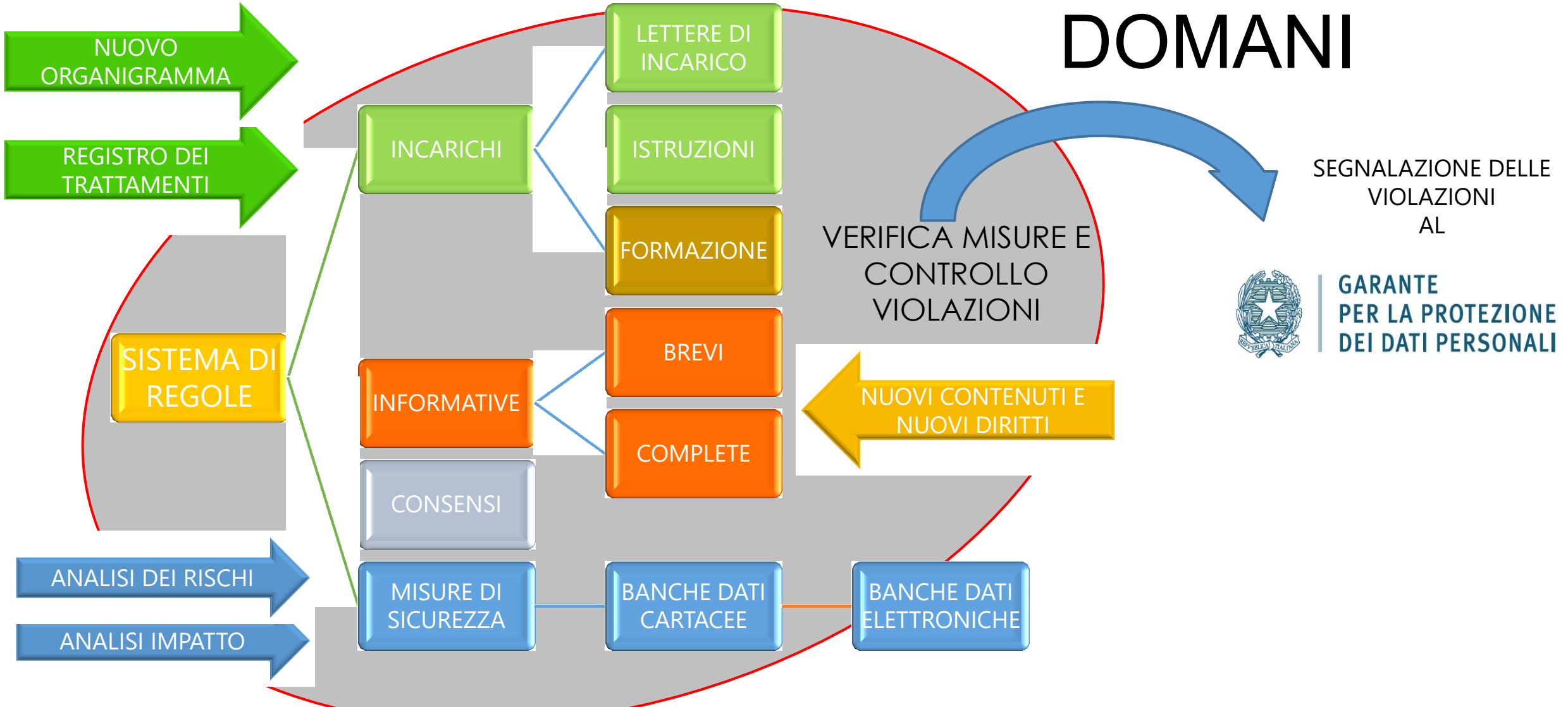
IL TITOLARE DEVE DEFINIRE UNA PROCEDURA PER TESTARE, VERIFICARE E VALUTARE REGOLARMENTE L'EFFICACIA DELLE MISURE INDIVIDUATE AL FINE DI GARANTIRE LA SICUREZZA DEL TRATTAMENTO.

ARCHITETTURA del sistema privacy

OGGI



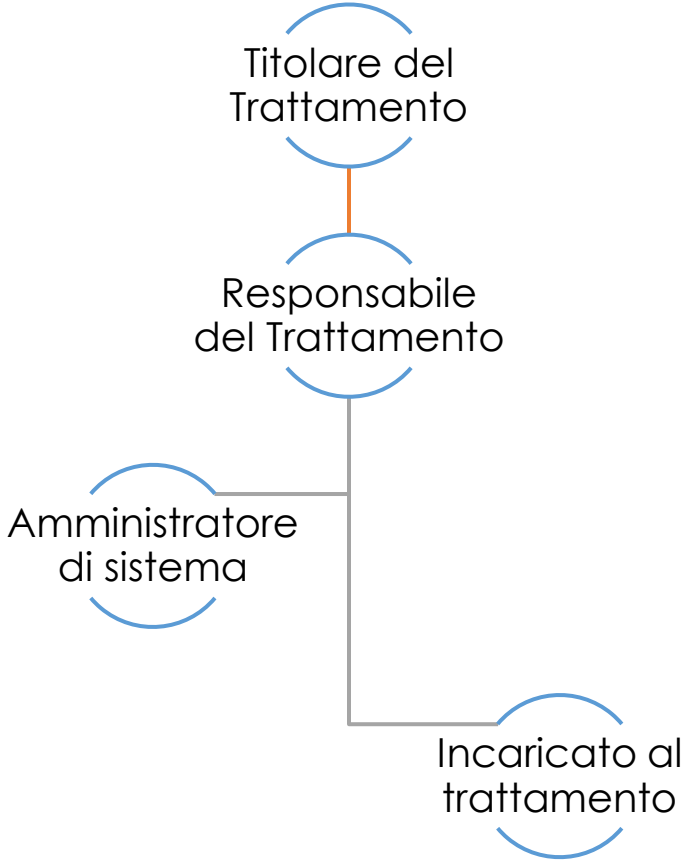
ARCHITETTURA del NUOVO sistema privacy



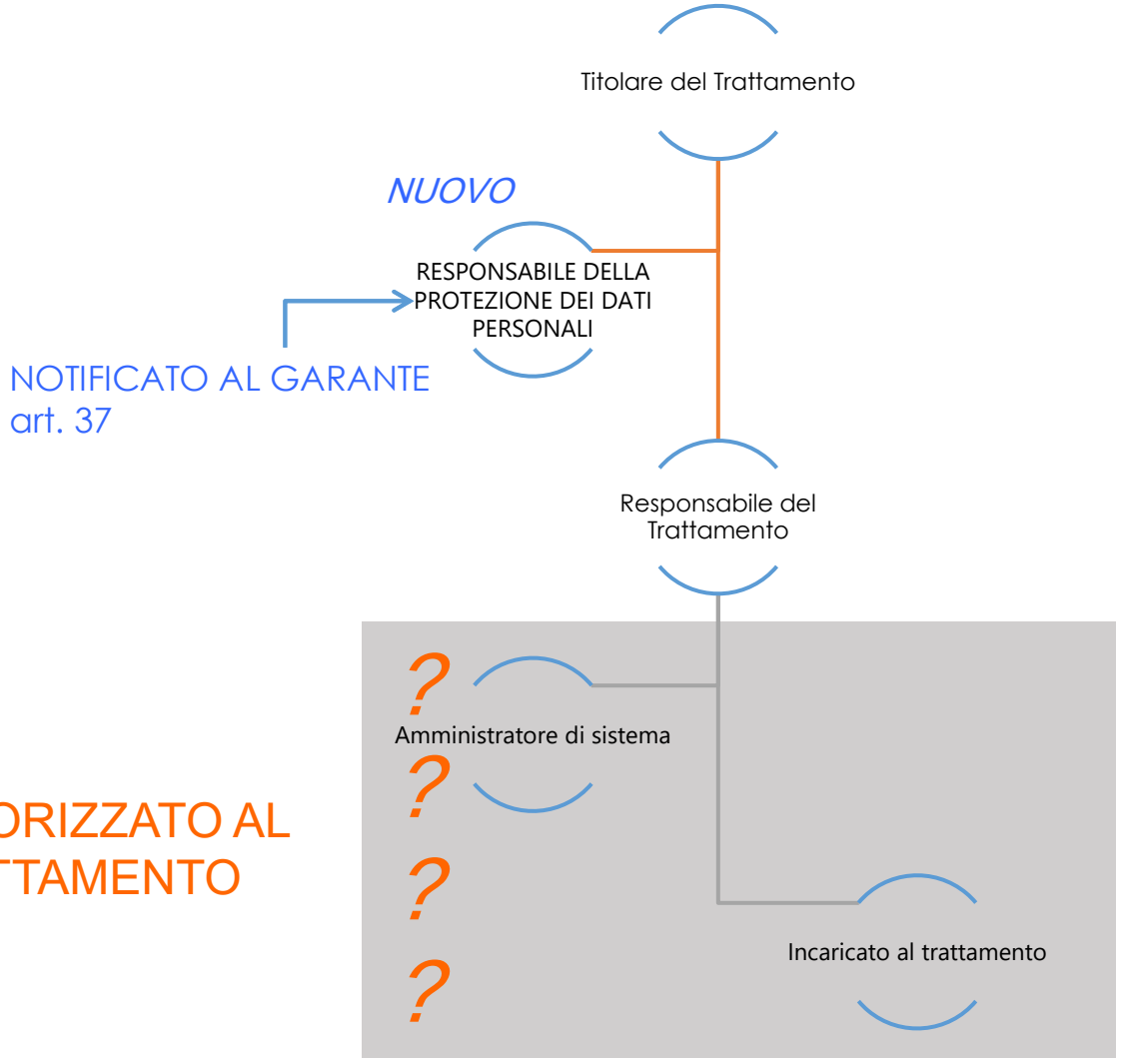
NUOVO ORGANIGRAMMA

UN NUOVO ORGANIGRAMMA

L' ORGANIGRAMMA PRIVACY OGGI



L' ORGANIGRAMMA PRIVACY DOMANI



AUTORIZZATO AL TRATTAMENTO

UN NUOVO ORGANIGRAMMA

TITOLARE DEL TRATTAMENTO: QUALI NOVITA'?

CHI E'?

E' la figura che determina le finalità ed
i mezzi del trattamento dei dati personali, tenuto conto di natura, ambito di applicazione e contesto.

QUALI SONO I SUOI COMPITI?

- Adottare misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento sia effettuato conformemente al Regolamento;
- Riesaminare periodicamente le misure tecniche e organizzative individuate e aggiornarle qualora necessario.

QUALI SONO LE SUE RESPONSABILITA'?

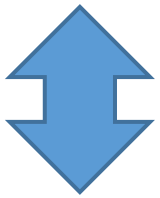
Tale figura risponderà per il danno cagionato dal trattamento dei dati personali realizzato in violazione del regolamento.

Il TITOLARE

UN NUOVO ORGANIGRAMMA

TITOLARE DEL TRATTAMENTO: QUALI NOVITA'?

Il TITOLARE



COTITOLARE

ACCORDO INTERNO
Definisce le rispettive responsabilità con particolare riguardo all'esercizio dei diritti dell'interessato e le rispettive funzioni di comunicazione delle informazioni.

CHI E'?
E' un partner del Titolare con cui, a fronte di un progetto comune, concorda e determina le finalità ed
i mezzi del trattamento dei dati personali tenuto conto di natura,
ambito di applicazione e
contesto.

UN NUOVO ORGANIGRAMMA

IL RESPONSABILE DEL TRATTAMENTO: QUALI NOVITA'?

CHI E'?

E' la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

QUALI SONO I SUOI COMPITI?

- Rispettare i termini e le istruzioni fornite tramite accordo scritto con il Titolare del Trattamento;
- Assicurare la riservatezza del personale autorizzato;
- Assistere il Titolare negli adempimenti previsti dal Regolamento;
- Segnalare al Titolare eventuali violazioni del Regolamento;
- Segnalare l'eventuale coinvolgimento di altri Responsabili del Trattamento;
- Dimostrare il rispetto dei propri obblighi e contribuire alle attività di revisione realizzate dal Titolare

Il RESPONSABILE DEL TRATTAMENTO

QUALI SONO LE SUE RESPONSABILITA'?

Tale figura risponderà per il danno causato dal trattamento solo se non ha adempiuto correttamente agli obblighi sanciti nel GDPR in capo ai responsabili del trattamento, oppure se ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.

UN NUOVO ORGANIGRAMMA

IL RESPONSABILE DEL TRATTAMENTO: QUALI NOVITA'?

a. NON è PIU' UNA FIGURA FACOLTATIVA
b. I trattamenti da parte del Responsabile sono disciplinati da un CONTRATTO, o da altro atto giuridico, in FORMA SCRITTA (anche in formato elettronico)

CONTENUTI DEL CONTRATTO

- 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.
- Le funzioni attribuite

UN NUOVO ORGANIGRAMMA

LA FIGURA DEL PRIVACY OFFICER O RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI

CHI E'?

una nuova figura aziendale, assolutamente indipendente e deputata a sorvegliare l'osservanza degli obblighi sulla protezione dei dati posti in capo al titolare o al responsabile del trattamento.

UN NUOVO ORGANIGRAMMA

LA FIGURA DEL PRIVACY OFFICER O RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI

QUANDO ADOTTARLO?

- Il Trattamento è effettuato da un'autorità pubblica o da un organismo pubblico
- MONITORAGGIO REGOLARE E SISTEMATICO DEGLI INTERESSATI SU LARGA SCALA
- Trattamento, su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali ed a reati

UN NUOVO ORGANIGRAMMA

LA FIGURA DEL PRIVACY OFFICER

QUALI SONO I SUOI COMPITI?

1) **INFORMARE** e fornire consulenza
2) **SORVEGLIARE** l'osservanza del regolamento
3) **FORNIRE**, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e **SORVEGLIARNE** lo svolgimento
4) **SUPPORTARE** il titolare o il responsabile anche nella tenuta di un registro delle attività di trattamento
5) **COOPERARE** con l'autorità di controllo e fungere da punto di contatto per questioni connesse al trattamento, tra cui la consultazione preventiva (ex verifica preliminare).

UN NUOVO ORGANIGRAMMA

LA FIGURA DEL PRIVACY OFFICER

QUAL E' LA SUA POSIZIONE E QUALI SONO I SUOI POTERI?

- Riferisce direttamente al vertice gerarchico del Titolare o del Responsabile del trattamento
- E' la figura di contatto per tutti gli interessati relativamente alle questioni legate al trattamento dei dati personali e all'esercizio dei loro diritti.
- NON DEVE RICEVERE ISTRUZIONI (interferenze) circa l'adempimento dei propri compiti
- NON DEVE ASSUMERE RUOLI CHE LO PONGANO IN CONFLITTO D'INTERESSE
- BUDGET DI SPESA AUTONOMO per assolvere ai compiti, accedere ai dati personali eD ai trattamenti e per mantenere la propria conoscenza specialistica
- Non può essere penalizzato o rimosso per l'adempimento dei propri compiti
- E' tenuto al segreto o alla riservatezza

UN NUOVO ORGANIGRAMMA

L'INCARICATO AL TRATTAMENTO

CHI E'?

Indica la persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile.

Tale figura è tenuta a rispettare gli ambiti di trattamento consentiti dal Titolare del Trattamento, e osservare le istruzioni fornite.

L'AMMINISTRATORE DI SISTEMA

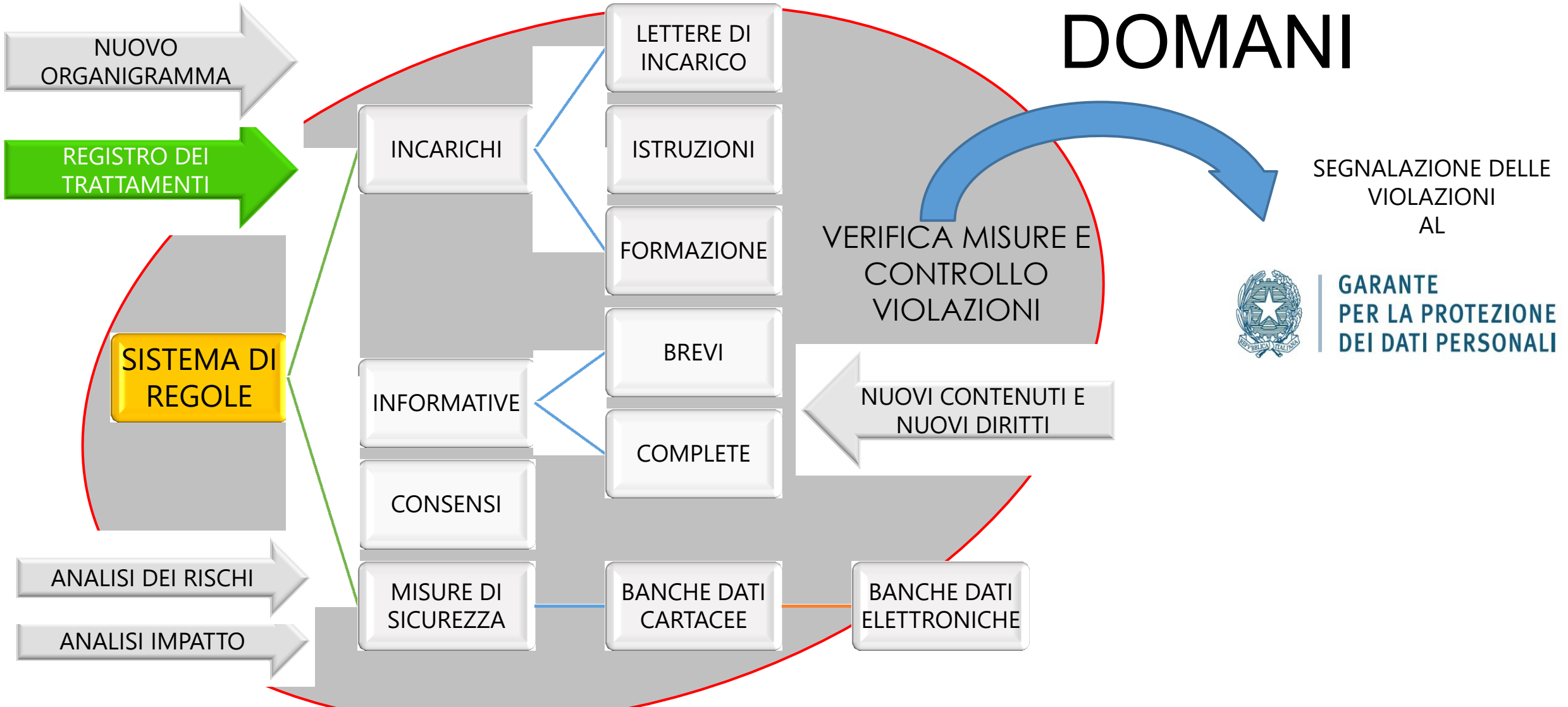
CHI E'?

indica le figure professionali incaricate della gestione e manutenzione dei sistemi informativi, di suoi componenti o parti di questo quali reti, apparati di sicurezza e sistemi software complessi

IL COMPITO DEL TITOLARE E DEL RESPONSABILE DEL TRATTAMENTO

- Valutare le competenze dell'AdS secondo criteri oggettivi e basati su evidenze documentali;
- Procedere alla loro designazione in modo individuale, elencando in modo analitico gli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;
- Tenere traccia degli estremi identificativi dell'AdS;
- Verificarne periodicamente l'operato;
- tracciare gli accessi dell' AdS per almeno sei mesi;
- Assicurarne nel tempo le conoscenze e competenze in materia di tutela e sicurezza dei dati personali.

ARCHITETTURA del NUOVO sistema privacy



IL REGISTRO DEI TRATTAMENTI

REGISTRO DEL TITOLARE DEL TRATTAMENTO

- Titolari/co-titolari del Trattamento
- Responsabile della Protezione dei Dati personali
- Le finalità del trattamento
- Categorie di interessati e di dati personali
- Categorie di destinatari
- Paese Terzo o Organizzazione Internazionale destinatari e relative garanzie;
- I termini ultimi previsti per la cancellazione delle diverse categorie di dati
- Una descrizione generale delle misure di sicurezza tecniche e organizzative

REGISTRO DEL RESPONSABILE DEL TRATTAMENTO

- I dati di contatto del responsabile o dei responsabili del trattamento di ogni titolare del trattamento per conto del quale agisce;
- Le categorie dei trattamenti effettuati per conto del titolare del trattamento;
- Paese Terzo o Organizzazione Internazionale destinatari e relative garanzie;
- Una descrizione generale delle misure di sicurezza tecniche e organizzative

Attenzione le AUTORIZZAZIONI concesse devono corrispondere agli ambiti di trattamento dei dati descritti nel registro!

IL REGISTRO DEI TRATTAMENTI

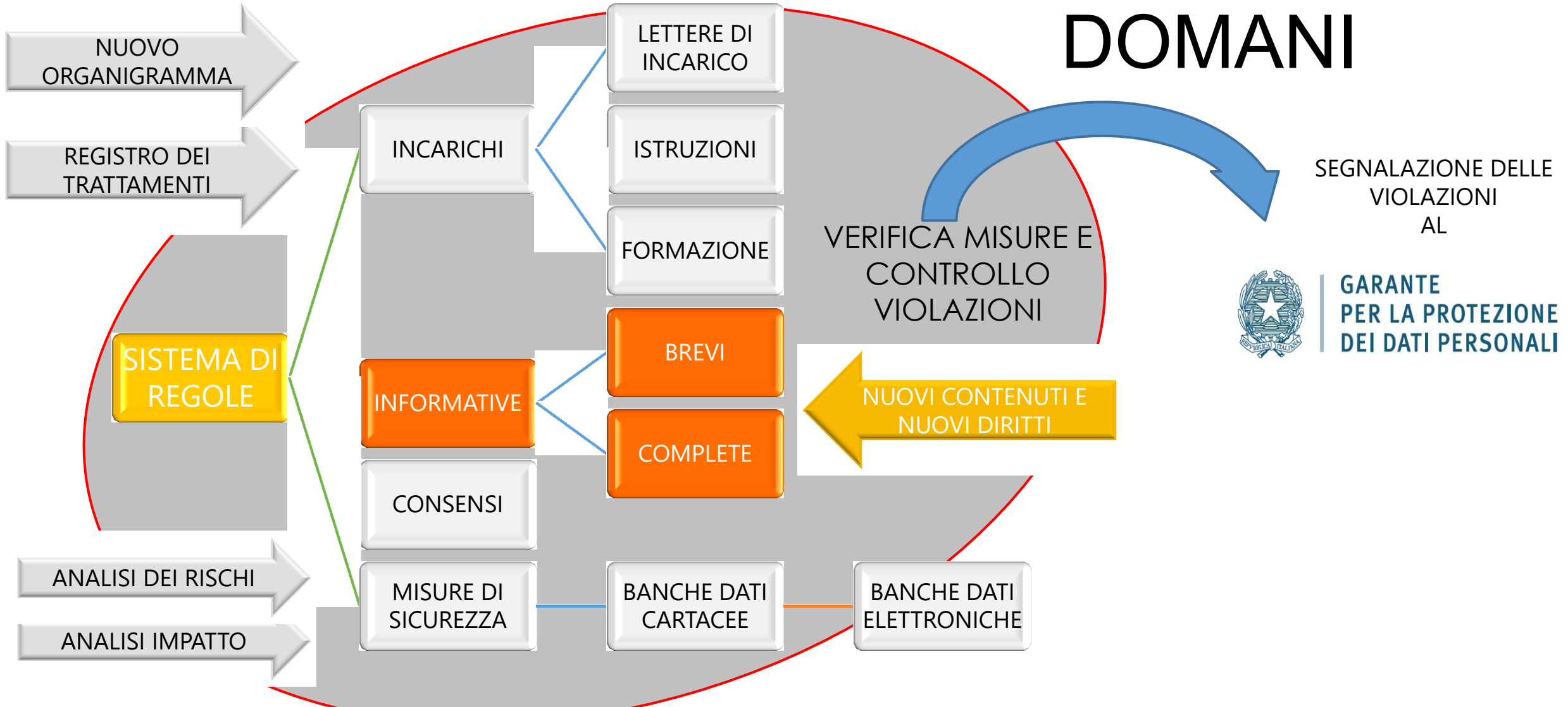
A. TUTTE LE AZIENDE CON PIÙ DI 250 DIPENDENTI

B. LE IMPRESE O ORGANIZZAZIONI CON MENO DI 250 DIPENDENTI SE:

1) il trattamento che esse effettuano IN MODO NON OCCASIONALE, può presentare un RISCHIO PER I DIRITTI E LE LIBERTA' DELL'INTERESSATO

2) Il trattamento include il trattamento NON OCCASIONALE dei dati particolari (sensibili e biometrici) o dati personali relativi a condanne penali e a reati.

ARCHITETTURA del NUOVO sistema privacy



UNA NUOVA INFORMATIVA

UNA NUOVA INFORMATIVA

L'informativa è il documento attraverso cui le organizzazioni rendicontano le proprie politiche privacy ed è considerato uno dei diritti dell'interessato in materia di privacy.

QUALI sono i suoi contenuti minimi?

UNA NUOVA INFORMATIVA: QUALI CONTENUTI MINIMI?

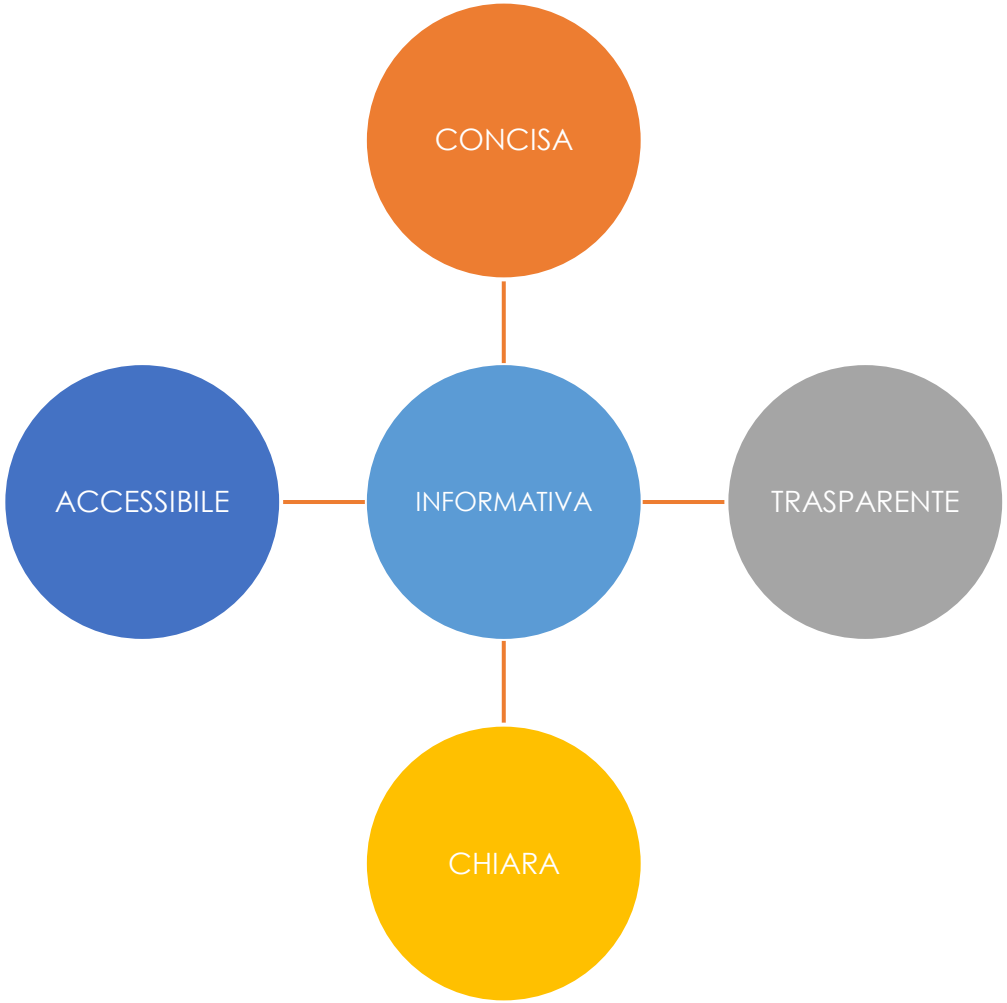
DATI RACCOLTI PRESSO L'INTERESSATO

1. Se previsto i dati di contatto del Privacy Officer
2. Le finalità del trattamento e **LA BASE GIURIDICA del trattamento**
3. **I LEGITTIMI INTERESSI** perseguiti dal titolare (ove applicabile)
4. I tempi di custodia o i criteri stabiliti
5. **L'intenzione del Titolare del trattamento di trasferire dati** personali a un Paese terzo o ad un'organizzazione internazionale (ove applicabile)* e con quali strumenti
6. I nuovi diritti
7. Effetti di sistemi di trattamento automatici (anche di profilazione) sull' l'interessato

DATI NON RACCOLTI PRESSO L'INTERESSATO

1) le categorie di dati personali in questione
2) La Fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico

UNA NUOVA INFORMATIVA: QUALI CARATTERISTICHE?



UNA NUOVA INFORMATIVA: QUANDO FORNIRLA?

DATI RACCOLTI PRESSO L'INTERESSATO	DATI NON RACCOLTI PRESSO L'INTERESSATO
Prima di effettuare la raccolta dei dati	**Entro un termine ragionevole che non può superare 1 mese** dalla raccolta, oppure **al momento della comunicazione** (**NON** della registrazione) dei dati (a terzi o all'interessato)

OGNI VOLTA CHE LE FINALITÀ CAMBIANO BISOGNA INFORMARE L'INTERESSATO

I PRINCIPALI DIRITTI DELL'INTERESSATO

- ACCESSO
- MODIFICA/RETTIFICA
- CANCELLAZIONE/OBLIO
- OPPOSIZIONE
- PORTABILITA'
- LIMITAZIONE

I PRINCIPALI DIRITTI DELL'INTERESSATO

FOCUS SUL DIRITTO DI CANCELLAZIONE:

Quando si può esercitare il diritto di cancellazione?

a) I dati non sono più necessari rispetto alla finalità di raccolta

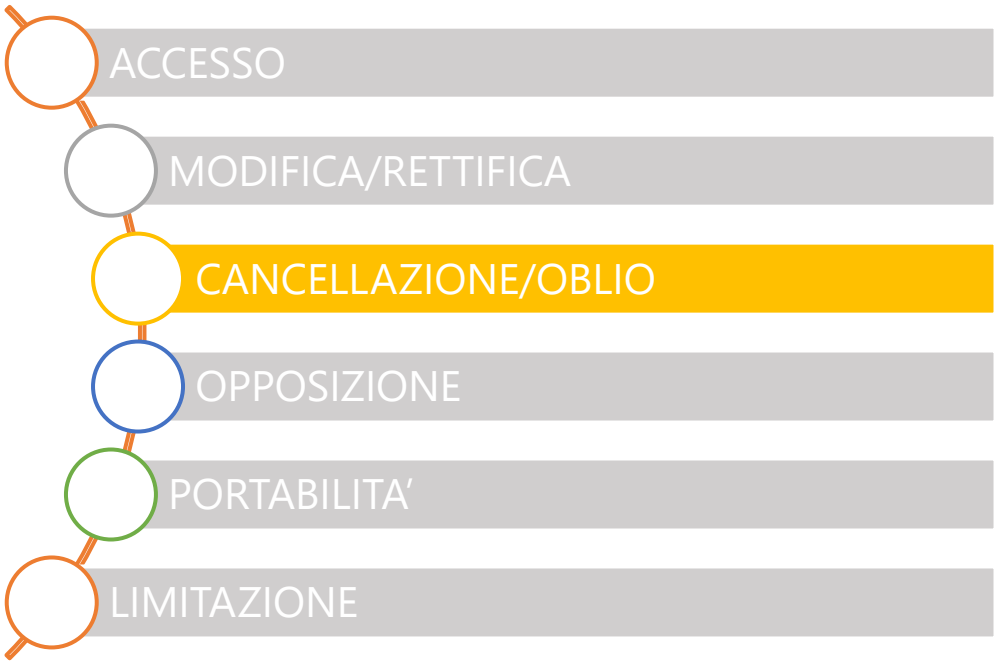
b) L'Interessato revoca il consenso e non c'è un altro presupposto di liceità

c) L'Interessato si oppone al trattamento e non c'è un interesse legittimo prevalente del Titolare

d) I dati sono stati trattati illecitamente

e) I dati devono essere cancellati in base ad una norma europea o nazionale

f) I dati sono stati raccolti relativamente all'offerta di servizi della società dell'informazione



I PRINCIPALI DIRITTI DELL'INTERESSATO

Il **diritto di opposizione** può essere esercitato:

a) per motivi legittimi;

b) quando i dati sono trattati per finalità commerciali o di marketing.

I PRINCIPALI DIRITTI DELL'INTERESSATO

DIRITTO ALLA PORTABILITA'

L'interessato può ricevere TUTTI i dati personali che lo riguardano in un formato:

- STRUTTURATO DI USO COMUNE.
- INTEROPERABILE.

per i trattamenti autorizzati tramite:

- CONSENSO dell'interessato
- CONTRATTO

I PRINCIPALI DIRITTI DELL'INTERESSATO

DIRITTO ALLA LIMITAZIONE

L'interessato può imporre delle «restrizioni» se:

- **contesta l'esattezza** dei dati personali;
- Il trattamento è illecito e l'interessato si **oppone alla cancellazione** dei dati personali
- i dati personali sono **necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria**

I PRINCIPALI DIRITTI DELL'INTERESSATO

Se il trattamento è **LIMITATO**, deve essere CONTRASSEGNATO E PUO' ESSERE UTILIZZATO SOLO:

- con il consenso dell'interessato
- per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria
- per tutelare i diritti di un'altra persona fisica o giuridica
- per motivi di interesse pubblico

I PRINCIPALI DIRITTI DELL'INTERESSATO

LIMITI ALL'ESERCIZIO DEI DIRITTI

- Vincoli legislativi;
- Tutela di un legittimo interesse del Titolare in sede giudiziaria;
- Il trattamento dei dati per pubblico interesse o nell'esercizio di pubblici poteri.

I PRINCIPALI DIRITTI DELL'INTERESSATO

TEMPI DI RISCONTRO

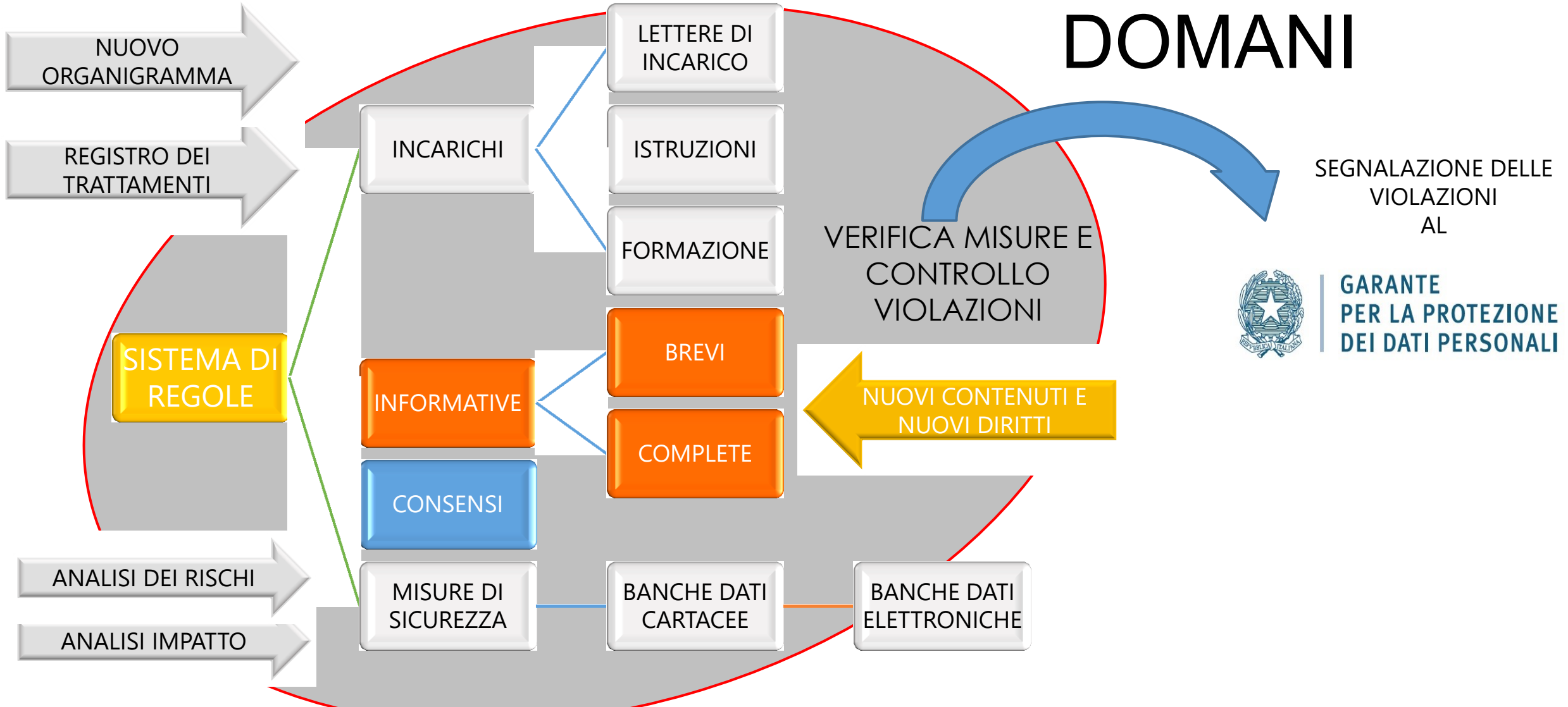
1 mese, estendibili fino a 3 mesi

IL TITOLARE DEVE COMUNQUE DARE UN RISCONTRO ALL'INTERESSATO ENTRO 1 MESE DALLA RICHIESTA, ANCHE IN CASO DI DINIEGO

MODALITA' DI RISCONTRO

- **SCRITTO**
- **ORALE**

ARCHITETTURA del NUOVO sistema privacy



IL CONSENSO


CONDIZIONI PER IL CONSENSO
POSITIVO
LIBERO
SPECIFICO
INFORMATO
INEQUIVOCABILE

IL CONSENSO

La richiesta di consenso per essere valida deve essere:

- chiaramente distinguibile da altre richieste o dichiarazioni
- formulata con un linguaggio comprensibile, semplice e chiaro
- se l'interessato è un minore di 16 anni, rivolta a chi esercita la potestà genitoriale sul minore

IL CONSENSO

1. CONSENSO,
2. adempimento obblighi contrattuali,
3. interessi vitali della persona interessata o di terzi,
4. obblighi di legge cui è soggetto il titolare,
5. interesse pubblico o esercizio di pubblici poteri,
6. interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati

PRINCIPI DI LICEITA'