CONFINDUSTRIA BERGAMO

Bergamo, 10 aprile 2018

IL NUOVO REGOLAMENTO EUROPEO SULLA PRIVACY
secondo incontro

Dott. Marco Invidiata
- Area lavoro e previdenza -
Confindustria Bergamo
035.275.235
m.invidiata@confindustriabergamo.it

Entrata in vigore

Il regolamento Europeo sulla privacy 2016/679/UE è già in vigore dal 24 maggio del 2016, ma diventerà efficace il

La nuova disciplina abroga espressamente la direttiva 95/46/CE.

Ambito di applicazione

Il regolamento Europeo si applica in ogni caso di trattamento dei dati personali di persone fisiche effettuato in ambito Ue da parte di Titolari o responsabili che si trovino all'interno dell'Unione Europea o da parte di Titolari del trattamento che, pur trovandosi in ambito extra-Ue, offrano beni, prestino servizi o compiano attività di monitoraggio del comportamento degli interessati che si trovino all'interno di uno degli Stati membri dell'unione Europea.

CONFINDUSTRIA BERGAMO

Verso il GDPR...

Il 21 novembre è entrata in vigore la legge n. 163/2017 contenente la delega al Governo per l'adeguamento della normativa nazionale alle disposizioni del nuovo Regolamento Europeo sulla privacy (cfr. art. 13).
La delega prevedeva inizialmente il rispetto dei seguenti principi:
-Abrogazione delle disposizioni del Codice della privacy incompatibili con quelle del Regolamento;
- modifica del Codice della privacy limitatamente a quanto necessario per dare attuazione alle disposizioni del Regolamento non direttamente applicabili;
- coordinamento delle disposizioni vigenti in materia di protezione dei dati personali con quelle del Regolamento;
- prevedere, ove opportuno, il ricorso a specifici provvedimenti attuativi e integrativi adottati dal Garante in attuazione delle disposizioni non direttamente applicabili contenute nel Regolamento;
- adeguare il sistema sanzionatorio penale e amministrativo vigente alle disposizioni del Regolamento.

…Addio codice della privacy

Con un comunicato Stampa del 21.03 u.s. il Consiglio dei Ministri ha previsto l'abrogazione integrale del Codice della privacy.

La nuova disciplina in materia sarà rappresentata principalmente dalle disposizioni del suddetto Regolamento immediatamente applicabili e da quelle recate dallo schema di decreto volte ad armonizzare l'ordinamento interno al nuovo quadro normativo dell'Unione Europea in tema di tutela della *privacy*.

Lo schema di decreto attuativo

- Attribuzione al Garante Italiano del potere di emanare misure di semplificazione per le PMI;
- Previsione di una disciplina transitoria volta ad assicurare il riordino, previa consultazione pubblica, delle autorizzazioni generali del Garante e ad indirizzare l'interpretazione dei Provvedimenti dell'Autorità e a definire in maniera rapida i procedimenti davanti alla stessa;
- conferma del regime privacy previsto per i dati contenuti nei CV spontaneamente inviati;

DUBBI:

- l'art. 14 c.1 prevede la facoltà per i titolari e i responsabili di attribuire determinati compiti a soggetti specifici;

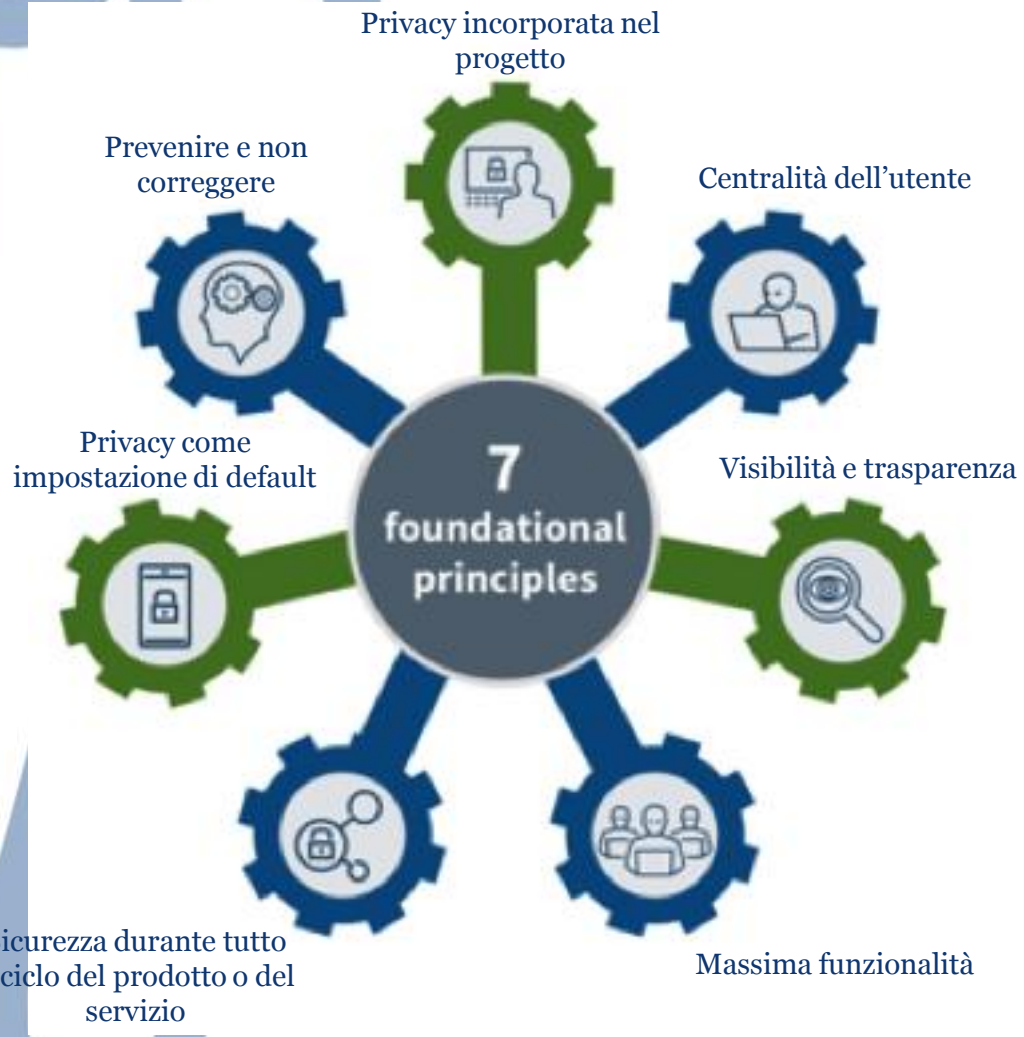
Accountability

"Responsabilizzazione" del Titolare del trattamento

CONFINDUSTRIA BERGAMO

Privacy by design (art. 25 c.1 GDPR)

Il Titolare del trattamento mette in atto misure tecniche e organizzative adeguate *«sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso»*.



CONFINDUSTRIA BERGAMO

Privacy by default (art . 25 c.2 GDPR)

«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 di trattamento».

PRIVACY BY DEFAULT

A CONCEPT FOR PRIVACY IN A WORLD WITH THE INTERNET OF THINGS

Quantità dei dati

Accessibilità

Portata del trattamento

Periodo di conservazione

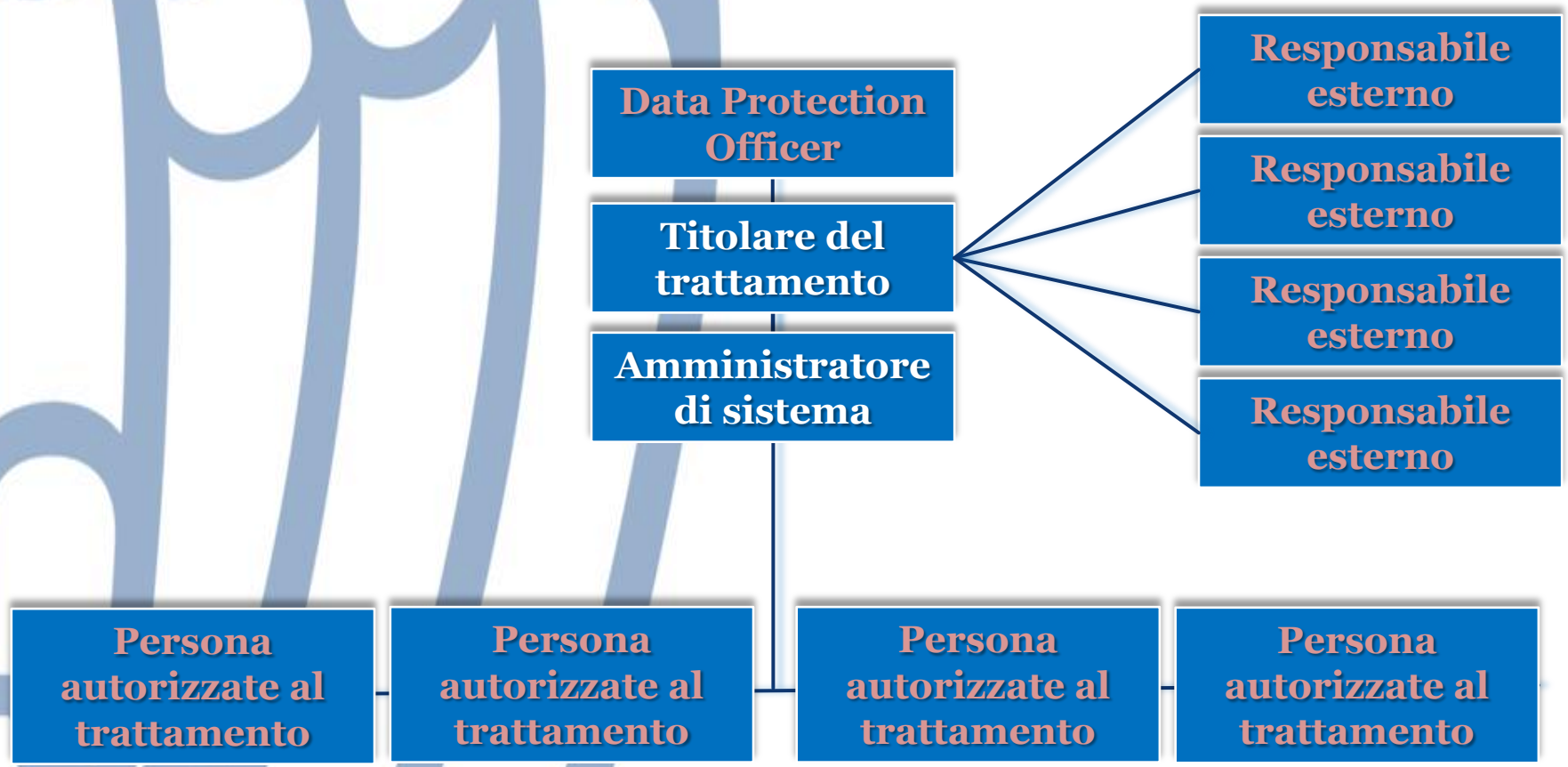
… le misure di sicurezza

ART. 24 Reg. 2016/679/UE: "*(…) il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il Trattamento è effettuato conformemente al (…) Regolamento. Dette misure sono riesaminate e aggiornate qualora necessario*". Inoltre "*se ciò è proporzionato rispetto alle attività di trattamento, le (predette) misure includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del responsabile del trattamento.*

ART. 32 Reg. 2016/679/UE:

-Stato dell'arte;
- Costi di attuazione;
- Natura del trattamento;
- Oggetto del trattamento;
- Contesto;
- Finalità;
- Rischio per i diritti degli interessati (probabilità che si verifichi un evento dannoso e conseguenze);

L’organigramma privacy: elementi di novità



CONFINDUSTRIA BERGAMO

Le persone autorizzate al trattamento

Art. 4 c. 10 → parla di persone autorizzate al trattamento dei dati sotto l'autorità diretta del titolare o del responsabile del trattamento.

Art. 29 "*Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso ai 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*".

Art. 28 c.3 c): è necessario che il responsabile del trattamento "*garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza*".

È opportuno continuare a fornire le istruzioni normalmente impartite attraverso la lettera di nomina ad incaricato del trattamento anche alle persone autorizzate.

Il responsabile del trattamento (esterno)

"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 c. 2 num.8)

NOMINA

responsabile

rappresentante

Contratto

Altro atto giuridico a norma del diritto Ue

RESPONSABILITÀ

Non ha adempiuto agli obblighi del regolamento a suo carico

Ha agito in maniera difforme rispetto alle istruzioni del titolare

CONFINDUSTRIA BERGAMO

Il flusso del dato

Interessato

Raccoglie

Dato personale

Fornisce l'informativa

Titolare del trattamento

Affida in outsourcing

Dato personale

Nomina responsabile esterno

Responsabile esterno

- Medico competente;
- Studio paghe;
- Banche (erogazione stipendi);
- Commercialista;
- Società fornitrici di servizi di archiviazione;
- Società di manutenzione software (in caso di accesso ad archivi);
- Rspp e ODV (esterni)
- (…)

Il contratto di nomina a responsabile del trattamento

CONFINDUSTRIA BERGAMO

Elementi da inserire nel contratto di nomina

-materia oggetto di trattamento;

- durata del trattamento;

- natura del trattamento;

- finalità del trattamento;

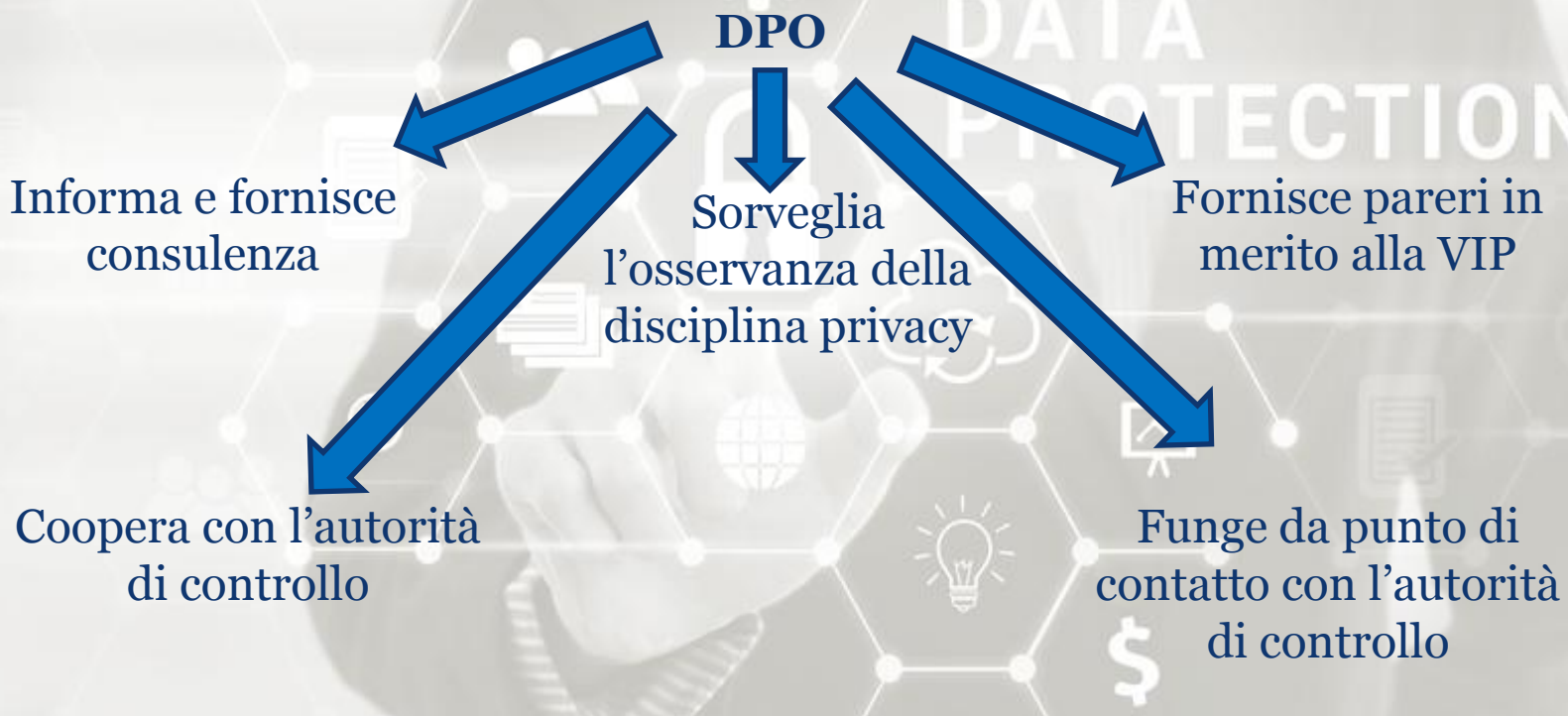
- tipologia di dati personali oggetto del trattamento;

- categorie di interessati;

- obblighi e diritti del titolare del trattamento.

Il responsabile per la protezione dei dati (RPD/DPO)…

"è una persona designata in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa (gdpr) e delle prassi nazionali ede europee, nonché della capacità di assolvere ai propri compiti" (art. 38 Reg. 679/2016/UE)



… quando va nominato?

Il DPO va nominato obbligatoriamente quando si verifichi una delle seguenti situazioni:

TRATTAMENTI:

- Effettuati da un'autorità pubblica
- Che per loro natura, finalità, ambito di applicazione consistano nel monitoraggio regolare e sistematico degli interessati su larga scala
- Effettuati su larga scala di dati sensibili o giudiziali

N.B. Affinché sussista l'obbligo di nominare il DPO è necessario che il trattamento costituisca attività principale del titolare del trattamento

Le faq del Garante italiano sul DPO

- Conferma della non necessità di un titolo specialistico per il DPO (faq n.2)
- deve poter disporre, infine, di risorse (personale, locali, attrezzature, ecc.) necessarie per l'espletamento dei propri compiti;
- **non è obbligatoria** la nomina del DPO (ad esempio, in relazione a trattamenti effettuati da liberi professionisti operanti in forma individuale; agenti, rappresentanti e mediatori operanti non su larga scala; imprese individuali o familiari; piccole e medie imprese, con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti;
- Conferma la possibilità di un unico DPO per gruppi di imprese;
- Conferma della possibilità di nomina interna ma non in conflitto di interesse;
- Sono **obbligati** a nominare il dpo (a titolo esemplificativo): istituti di credito; imprese assicurative; sistemi di informazione creditizia; società finanziarie; società di informazioni commerciali; società di revisione contabile; società di recupero crediti; istituti di vigilanza; partiti e movimenti politici; sindacati; caf e patronati; società operanti nel settore delle "utilities" (telecomunicazioni, distribuzione di energia elettrica o gas); imprese di somministrazione di lavoro e ricerca del personale; società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione; società di call center; società che forniscono servizi informatici; società che erogano servizi televisivi a pagamento

I nuovi adempimenti

INFORMATIVA E BASE GIURIDICA DEL TRATTAMENTO

I DIRITTI DELL'INTERESSATO

LA VALUTAZIONE D'IMPATTO PRIVACY

IL REGISTRO DEI TRATTAMENTI

LA PROCEDURA DI DATA BREACH

Gli elementi essenziali dell'informativa e …

Informativa
Dati raccolti c/o l'interessato

si → *Prima di effettuare la raccolta dei dati (art.13)*

no → *Entro un termine ragionevole (inferiore a 1 mese);*

Art. 13 d.lgs. 196/03

-Finalità del trattamento
- natura obbligatoria o facoltativa del conferimento
- soggetti o categorie di soggetti a cui possono essere comunicati o venirne a conoscenza in qualità di responsabili
- ambito di diffusione e trasferimento;
- estremi identificativi del titolare e dei Responsabili nonché dell'ADS;
- diritti dell'interessato;

Novità Reg. 679/2016/UE

-base giuridica del trattamento;
- periodo di conservazione dei dati;
- indicazione del Paese terzo ai quali i dati sono trasferiti e attraverso quali strumenti;
- dati di contatto del DPO;
- diritto di presentare reclamo all'autorità di controllo;
- trattamento effettuato con processi decisionali automatizzati e attività di profilazione, indicando la logica di tali processi e le conseguenze per l'interessato;

Informativa e posta elettronica

Il Garante con il provv. N. 53/2018 ha sancito/ribadito i seguenti principi:

- l'azienda ha l'onere di **informare circa le modalità e le finalità di utilizzo della posta elettronica** (policy aziendale);
- Il datore di lavoro deve **informare** l'interessato riguardo le eventuali **operazioni condotte, sulla mail** a lui attribuita, dall'amministratore di sistema (es. lettura e-mail);
- Il datore di lavoro deve indicare **in che misura e con che modalità vengano effettuati i controlli** (Provv. 1° marzo 2007, n. 13: "Linee guida per posta elettronica e internet», art. 4 c. 3 st. lav.)
- **Impossibilità di archiviare le e-mail dei dipendenti a tempo indeterminato** o comunque per periodi ampi → necessità di predisporre sistemi di archiviazione documentale in grado di archiviare selettivamente i documenti (es. sistemi di protocollazione);
- **Disattivazione dell'account** del dipendente alla cessazione del rapporto di lavoro e rimozione della casella di posta elettronica del dipendente → attivazione di account alternativi;

… la base giuridica del trattamento

Il trattamento è lecito ex art. 6 del Regolamento se:

- si fonda sul CONSENSO dell'interessato;

- se compiuto per ADEMPIERE OBBLIGHI CONTRATTUALI o DI LEGGE;

- l'INTERESSE LEGITTIMO DEL TITOLARE O DI UN TERZO è prevalente rispetto al diritto dell'interessato;

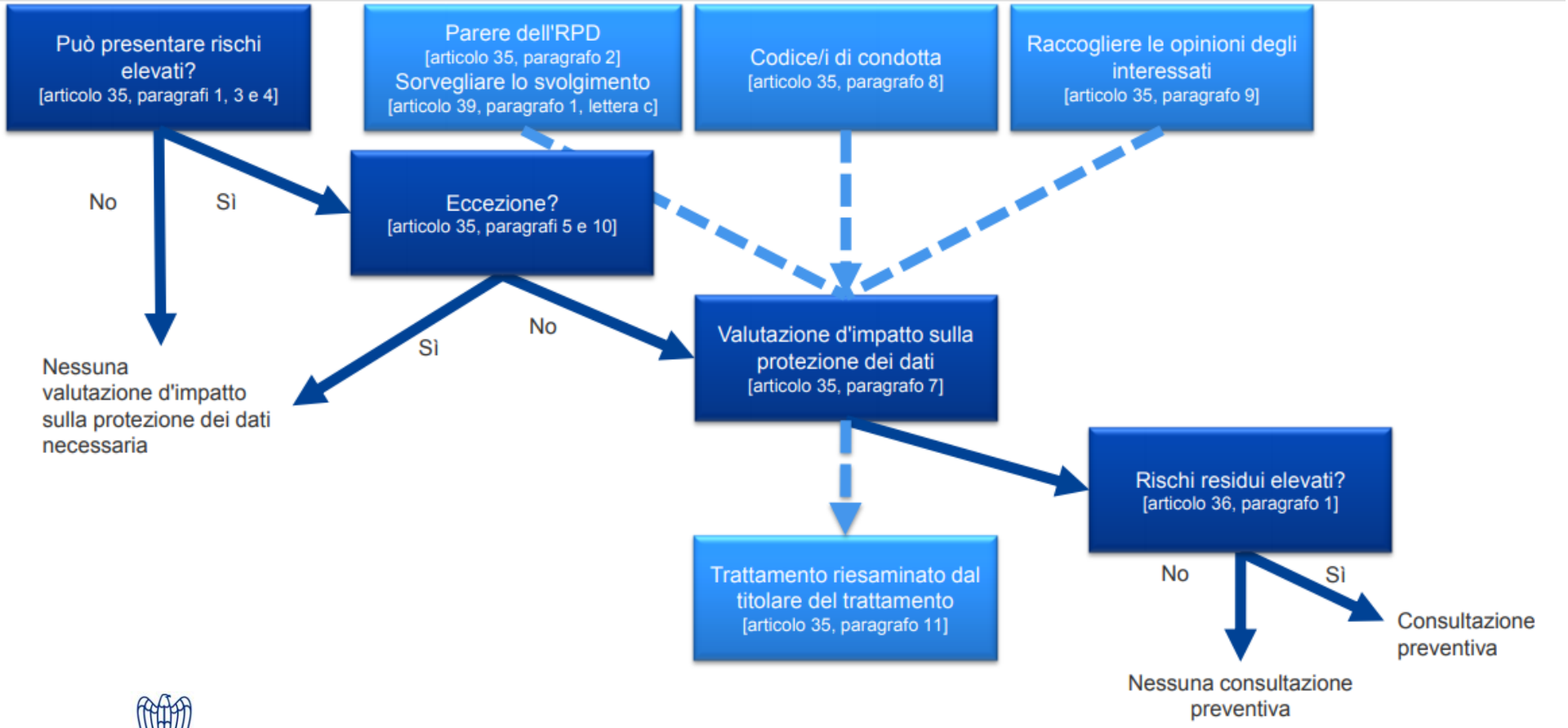
- effettuato finalità di PUBBLICO INTERESSE;

- effettuato nell'esercizio di PUBBLICI POTERI;

- È effettuato per SALVAGUARDARE UN INTERESSE VITALE DI UN TERZO;

La valutazione di impatto privacy (VIP/DPIA)

È necessario effettuare una valutazione di impatto sulla protezione dei dati personali solo quando il trattamento "*può presentare un rischio elevato per i diritti e le libertà delle persone fisiche*" (art. 35 p.1)



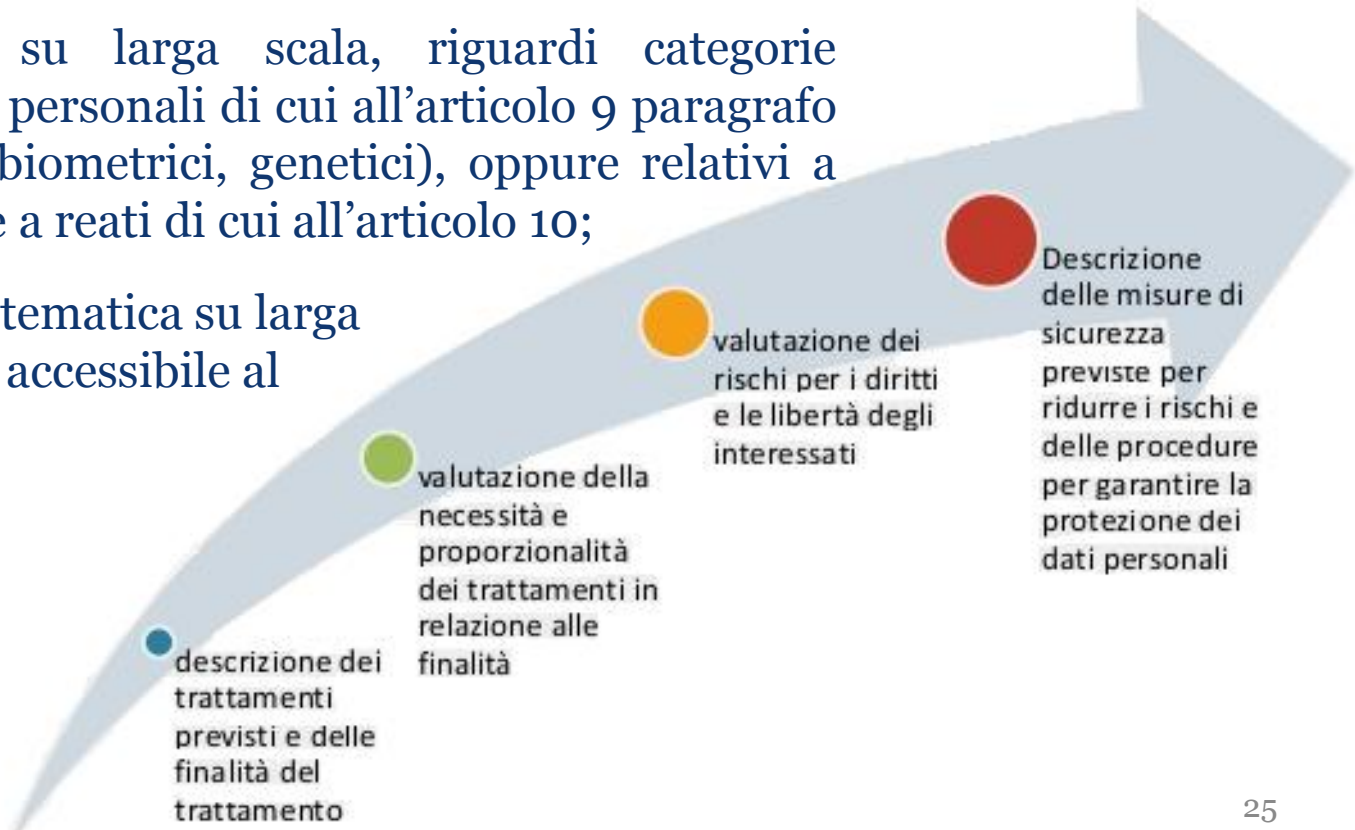
Obbligo di VIP ed elementi

La valutazione d'impatto sui dati personali è obbligatoria nei seguenti casi:

a) qualora il trattamento consista in un valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;

b) il trattamento, su larga scala, riguardi categorie particolari di dati personali di cui all'articolo 9 paragrafo 1 (dati sensibili, biometrici, genetici), oppure relativi a condanne penali e a reati di cui all'articolo 10;

c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico



Le Linee Guida del Garante sulla VIP

E' richiesta la VIP qualora il trattamento integri almeno 2 dei seguenti criteri:

1. Trattamento che riguardi aspetti quali "*il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato*";
2. Processi decisionali automatizzati che hanno effetti giuridici o che incidono in modo analogo sulle persone;
3. Monitoraggio sistematico;
4. Dati sensibili o dati aventi carattere altamente personale;
5. Trattamenti su larga scala;
6. Creazioni di corrispondenze o combinazione di insiemi di dati;
7. Dati relativi a interessati vulnerabili;
8. uso innovativo od applicazione di nuove soluzioni tecnologiche od organizzative;
9. quando il trattamento impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

La VIP richiede uno sforzo continuo

Registro dei trattamenti (art. 30 GDPR)

La compilazione di un registro del trattamento è obbligatoria solo per le imprese od organizzazioni con più di 250 dipendenti, oppure dal titolare che effettui trattamenti che possono presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o all'orientamento sessuale della persona, o i dati personali relativi a condanne penali o reati.

Contenuto del registro dei trattamenti

Indicazione Trattamento (es. dati del personale, dati dei CV, dati dei visitatori, dati personali raccolti da sito web, dati di clienti persone fisiche ecc....)

Finalità del trattamento

Categoria di interessati

Categoria di dati personali trattati

Categorie di destinatari a cui i dati possono essere comunicati

Trasferimento all'estero

Termine per la conservazione/cancellazione del dato

Descrizione delle misure di sicurezza

Prima di iniziare: Audit interno

Consiste in una valutazione dei processi aziendali sul grado di rispetto della normativa.

- Quali dati personali tratta l'azienda? A chi vengono comunicati? Come vengono archiviati?

- Per quale ragione/finalità sono stati richiesti?

- Sono davvero necessari questi dati?

- Quanto a lungo si conserveranno/tratteranno?

- Quale diritto (base giuridica) si ha di riceverli e di trattarli?

- Posso fornire lo stesso servizio senza richiedere tutti i dati raccolti?

- Quali sono i pericoli per l'interessato se a questi dati avessero accesso terzi o venissero cancellati?

- Quali misure sono prese per ridurre il rischio?

Descrizione attività di trattamento

Trattamento 1: [Descrizione]

1. **Tipologia di dati**
2. **Trattamento/Posizione dei dati**
3. **Trattamento/accesso ai dati**
4. **Conseguenze di una mancata registrazione del dato**
5. **Durata del trattamento**
6. **Formazione**
7. **Rischi e potenziale impatto sull'interessato**
8. **Interventi per minimizzare i dati o aumentare la loro sicurezza**
9. **Basi giuridiche per il trattamento**

GRAZIE PER L'ATTENZIONE

Dott. Marco Invidiata
- Area lavoro e previdenza -
Confindustria Bergamo
035.275.235
m.invidiata@confindustriabergamo.it

CONFINDUSTRIA BERGAMO