Centro Servizi Ingegneria

Integrated Consulting Services

MISURE DI SICUREZZA DEL TRATTAMENTO DEI DATI ADEGUATE AL CONTESTO DELLE ORGANIZZAZIONI AZIENDALI

Dott.sa Laura Pellegrino

13 dicembre 2018 ***CONFINDUSTRIA SALERNO***

Via Rosa Jemma, 2 - Centro Direzionale Pastena 84091 Battipaglia (SA)

Tel./Fax 0828/302630 Sito web: www.csisrl.com E-mail: csi@csisrl.com

REGOLAMENTO (EU) 2016/679

GDPR: General Data Protection Regulation

Quali sono le misure di sicurezza da adottare e cosa è cambiato con le novità introdotte dal Regolamento europeo?

Centro Servizi Ingegneria
Integrated Consulting Services

Sicurezza del trattamento (art.32)

"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"

Stato dell'arte e costi di attuazione

Natura, oggetto, contesto e finalità del trattamento **Rischio per i diritti e le libertà dell'interessato**

Adozione di misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio

Centro Servizi Ingegneria
Integrated Consulting Services

Sicurezza del trattamento (art.32)

Tali misure "adeguate" 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.

Misure di Sicurezza del trattamento

Pseudonimizzazione

un particolare trattamento dei dati volto a nascondere l'identità dell'interessato e a impedirne l'identificazione senza l'utilizzo di informazioni aggiuntive, per cui i dati stessi non potranno più essere attribuiti direttamente ed automaticamente ad un interessato specifico.

Cifratura

è una modalità di conversione dei dati in una sequenza apparentemente casuale di lettere, numeri e segni speciali che solo la persona in possesso della corretta chiave di decifratura potrà riconvertire nel file di testo originale, da realizzare attraverso l'utilizzo di meccanismi che normalmente prevedono l'impiego di algoritmi di crittografia.

Misure di Sicurezza del trattamento

La **Cifratura** dei dati e degli archivi e la **Pseudonimizzazione** delle informazioni sono considerate dal GDPR come tecniche idonee per garantire una reale protezione dei dati, soprattutto di quelli sensibili.

In un'eventuale fuga di questi dati, le informazioni reperibili sarebbero visibili ma assolutamente incomprensibili o destrutturate, ossia separate da altre informazioni che sarebbero in grado di dar loro un senso.

PRINCIPIO DI ACCOUNTABILITY

L'art.32 non elenca tassativamente le misure minime da adottare, ma affida ai titolari il compito di decidere autonomamente quali misure tecniche ed organizzative mettere in atto al fine di garantire un livello di sicurezza adeguato al rischio.

Il principio di accountability – "Responsabilizzazione" sta alla base del nuovo approccio promosso dal GDPR ed è inserito all'interno dell'art. 5 del Regolamento "Principi applicabili al trattamento di dati personali"

Centro Servizi Ingegneria
Integrated Consulting Services

PRINCIPI GENERALI

Devono essere rispettati in ogni fase del trattamento.

LICEITÀ CORRETTEZZA E TRASPARENZA:

Ogni trattamento è esplicitamente indicato nell'informativa

MINIMIZZAZIONE DEI DATI:

Adeguati, pertinenti e limitati

LIMITAZIONE DELLA CONSERVAZIONE:

Per un periodo temporale limitato al conseguimento delle finalità

LIMITAZIONE DELLE FINALITÀ:

Determinate, esplicite e legittime

ESATTEZZA:

I dati devono essere Esatti e, se necessario, aggiornati

INTEGRITÀ E RISERVATEZZA:

Deve essere garantita un'adeguata sicurezza dei dati personali

"Il Titolare del trattamento è competente per il rispetto del paragrafo 1 ed in grado di dimostrarlo" (art. 5.2)

Centro Servizi Ingegneria
Integrated Consulting Services

Responsabilità del Titolare del trattamento (art. 24)

E ancora

"Tenuto conto…….il Titolare del trattamento mette in atto misure tecniche ed organizzative adeguate per garantire ed essere in grado **di dimostrare** che il trattamento è effettuato conformemente al presente regolamento"

ACCOUNTABILITY (RESPONSABILIZZAZIONE) & RENDICONTAZIONE

Non basta aver adempiuto alle richieste normative, ma **occorre essere in grado di dimostrarlo**

Centro Servizi Ingegneria
Integrated Consulting Services

PRIVACY BY DESIGN E PRIVACY BY DEFAULT

Al fine di poter dimostrare la **conformità** con il GDPR il titolare adotta **politiche interne** e attua **misure** che soddisfano in particolare i principi della **protezione dei dati fin dalla progettazione** e della **protezione dei dati di default.**

PRIVACY BY DESIGN E BY DEFAULT (Nuovi Criteri)

Il Regolamento introduce il principio di «**privacy by design** » -o di «protezione dei dati personali fin dalla progettazione» - prevede che ogni titolare o responsabile del trattamento debba tenere in considerazione, sin dalla ideazione e progettazione delle attività di trattamento, i principi di protezione dei dati al fine di soddisfare i requisiti del regolamento e tutelare i diritti degli interessati (art. 25 c.1).

Pertanto, le attività, i prodotti e i servizi che comportano il trattamento di dati personali devono essere progettati e sviluppati in modo da assicurare il rispetto dei principi e delle garanzie a tutela della privacy, ad esempio prevedendo misure per minimizzare l'utilizzo di dati personali.

Centro Servizi Ingegneria
Integrated Consulting Services

PRIVACY BY DESIGN E BY DEFAULT (Nuovi Criteri)

Principio di «**privacy by default**» - o di «protezione dei dati personali «per impostazione predefinita» - prevede che ogni titolare o responsabile effettui il trattamento dei soli dati personali degli interessati nella misura e per il tempo necessario a raggiungere le specifiche finalità del trattamento, implementando, all'interno degli ambienti, dei sistemi informatici e delle infrastrutture di rete utilizzate per tale trattamento, le misure tecniche idonee a proteggere i dati personali degli interessati (art. 25 c.2).

Pertanto, devono essere adottati meccanismi (di natura informatica e gestionale) che assicurano che per impostazione predefinita:

- Siano utilizzati solo i dati necessari a uno scopo specifico;
- Non siano resi disponibili i dati personali ad un numero indefinito di persone;
- I dati non siano archiviati oltre il tempo necessario alla finalità del trattamento.

Centro Servizi Ingegneria
Integrated Consulting Services

PRIVACY BY DESIGN E PRIVACY BY DEFAULT

L'applicazione del principio di «**privacy by design e by default**» implica la necessità di configurare il trattamento prevedendo **fin dall'inizio** le garanzie indispensabili al fine di soddisfare i requisiti del regolamento e tutelare i diritti degli interessati, **tenendo conto del contesto complessivo** ove il trattamento si colloca **e dei rischi** per i diritti e le libertà degli interessati.

E' necessario implementare dispositivi di sicurezza il prima possibile poiché ad uno stadio più avanzato essi si rivelerebbero insufficienti a garantire un'effettiva protezione dei diritti degli interessati.

Centro Servizi Ingegneria
Integrated Consulting Services

RISK BASED APPROACH

Il concetto di rischio permea l'intero Regolamento:

- Art. 5 par. 1 lett. f), par 2 - Principi applicabili al trattamento di dati personali e competenza del titolare;
- art. 24 Responsabilità del titolare del trattamento;
- art. 25 Privacy by design e privacy by default;
- Art. 28 par. 3 lett. e) Responsabile del trattamento;
- Art. 32 Sicurezza del trattamento;
- Art. 33 par. 3 lett. c) - Notifica di una violazione dei dati personali all'autorità di controllo;
- Art. 35 par. 1, 7 lett. c) e d) Valutazione d'impatto sulla protezione dei dati;
- Art. 39 par 2 Compiti del responsabile della protezione dei dati

RISK BASED APPROACH

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.

Dunque occorre tutelare i dati personali in termini di:

- Riservatezza;
- Autenticità (esattezza);
- Integrità;
- Disponibilità.

Centro Servizi Ingegneria
Integrated Consulting Services

GESTIONE DEL RISCHIO

Valutazione del Rischio

- Analisi del Rischio (Identificazione pericoli/eventi pericolosi, Individuazione della cause)
- Ponderazione del Rischio (determinazione livello di Rischio)

Trattamento del Rischio

- Mitigazione del Rischio (misure di prevenzione e protezione)
- Verifica e trattamento Rischio Residuo

Centro Servizi Ingegneria
Integrated Consulting Services

GESTIONE DEL RISCHIO

Identificazione pericoli/eventi pericolosi

L'identificazione dei pericoli è un'operazione che porta a definire tutti i pericoli, le situazioni e gli eventi pericolosi, associati alla specifica attività di trattamento di dati personali, che possano comportare esposizione a rischio per i diritti e le libertà delle persone fisiche.

Centro Servizi Ingegneria
Integrated Consulting Services

IDENTIFICAZIONE DEI PERICOLI

Comportamenti degli operatori:

- Sottrazione di credenziali di autenticazione;
- Carenza di consapevolezza, disattenzione o incuria;
- Comportamenti sleali o fraudolenti;
- Errore materiale;

Eventi relativi agli strumenti

Eventi relativi al contesto

Centro Servizi Ingegneria
Integrated Consulting Services

GESTIONE DEL RISCHIO

Eventi relativi agli strumenti:

- Azione di virus informatici o di programmi suscettibili di recare danno;
- Spamming o tecniche di sabotaggio;
- Malfunzionamento, indisponibilità o degrado degli strumenti;
- Accessi esterni non autorizzati;
- Intercettazione di informazioni in rete;

Eventi relativi al contesto:

- Eventi distruttivi, naturali o artificiali (terremoti, incendi, allagamenti, ecc.), nonché dolosi, accidentali o dovuti ad incuria;
- Guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.);
- Errori umani nella gestione della sicurezza fisica;

Centro Servizi Ingegneria
Integrated Consulting Services

PONDERAZIONE DEL RISCHIO

Per ogni evento pericoloso occorre individuare:

- frequenza: probabilità che l'evento si verifichi in un determinato intervallo di tempo;
- magnitudo: entità delle possibili perdite e dei danni conseguenti al verificarsi dell'evento.

Rischio = Frequenza x Magnitudo

TRATTAMENTO DEL RISCHIO

Quando il livello rischio potenziale assume valori significativi ovvero non è "tollerabile", è necessario adottare delle soluzioni che ne riducano la gravità del potenziale danno, attraverso l'adozione di:

- misure di sicurezza organizzative (impatto sulle procedure organizzative)
- misure di sicurezza fisiche (impatto sulla sicurezza strutturale)
- misure di sicurezza logiche (impatto sulla sicurezza informatica)

Centro Servizi Ingegneria
Integrated Consulting Services

MISURE DI SICUREZZA ORGANIZZATIVE

Ad esempio:

- Rilascio e revoca dell'autorizzazione da parte del Titolare o Responsabile agli incaricati per trattare i dati sensibili
- Previsione di diversi livelli di autorizzazione di accesso ai dati in relazione ai compiti e mansioni assegnate
- Verifica di validità delle autorizzazioni per l'accesso ai dati sensibili
- Istruzioni scritte per lo svolgimento dei compiti assegnati
- Verifica della restituzione dei documenti originali al termine delle operazioni affidate
- Previsione di interventi formativi per rendere edotti gli incaricati delle principali novità normative intervenute
- Modalità di interazione con gli interessati (accesso ai dati, opposizione, ecc.)

MISURE DI SICUREZZA FISICHE

Ad esempio:

- Archivio ad accesso selezionato e controllato
- Back- up sistematico dei dati.
- Dispositivi di allarme in archivi cartacei
- Sistemi antincendio in archivi cartacei
- Vigilanza esterna archivi
- Sistemi allarme in locali PC
- Dispositivi antintrusione in locali PC
- Dispositivi antincendio in locali PC
- Vigilanza esterna nei locali PC
- Gruppi di continuità

Centro Servizi Ingegneria
Integrated Consulting Services

MISURE DI SICUREZZA LOGICHE

Ad esempio:

- Codice identificativo personale univoco per l'accesso al PC
- Disattivazione del codice identificativo personale in caso di cambiamento/termine della mansione
- Password di almeno 8 caratteri e cambio periodico della stessa
- Predisposizione di istruzioni relative alla diligente custodia dell'elaboratore e della parola chiave
- Utilizzo di programmi anti-virus e loro aggiornamento
- Dispositivi per la limitazione dell'accesso a particolari siti web potenzialmente pericolosi (black list)

Centro Servizi Ingegneria
Integrated Consulting Services

ADEGUATEZZA MISURE DI SICUREZZA

L'adeguatezza delle misure di sicurezza ai rischi dovrà essere documentata da policy aziendali di sicurezza dei dati che andranno ad esplicitare le misure organizzative e comportamentali finalizzate al contrasto dei rischi.

Centro Servizi Ingegneria
Integrated Consulting Services

GESTIONE DEL RISCHIO

TIPOLOGIA	MINACCIA	VULNERABILITÀ	DANNO	CONTROMISURE
Comportamenti degli operatori	Furto di credenziali di autenticazione	Personale non formato. Strumenti non conformi;	Accesso o trattamento da parte di soggetti non autorizzati; Perdita totale o parziale dei dati; Alterazione delle informazioni.	• Formazione del personale. • Implementazione di una procedura per la nomina del custode delle password, • Adeguamento periodico parco macchine. • Aggiornamento dei sistemi operativi.
	Carenza di consapevolezza, disattenzione o incuria	Personale non formato	Accesso o trattamento da parte di soggetti non autorizzati	Formazione del personale. Consegna del mansionario per ciascun incaricato;

Centro Servizi Ingegneria
Integrated Consulting Services

GESTIONE DEL RISCHIO

TIPOLOGIA	MINACCIA	VULNERABILITÀ	DANNO	CONTROMISURE
Eventi relativi agli strumenti	Azione di virus informatici	Antivirus non aggiornato. Comportamenti scorretti	Perdita totale o parziale dei dati; accesso o trattamento da parte di soggetti non autorizzati.	• Formazione del personale. • Aggiornamento dei sistemi operativi;
	Spamming o altre tecniche di sabotaggio	Antivirus non aggiornato. Comportamenti scorretti	Perdita totale o parziale dei dati; accesso o trattamento da parte di soggetti non autorizzati.	• Formazione del personale. • Aggiornamento dei sistemi operativi.
	Malfunzionamento, indisponibilità o degrado degli strumenti	Risorse obsolete, strumenti non conformi, impianti elettrici non a norma.	Perdita totale o parziale dei dati; blocco operativo e perdita dell'integrità della banca dati.	• Adeguamento periodico parco macchine. • Aggiornamento dei sistemi operativi.

Centro Servizi Ingegneria
Integrated Consulting Services

GESTIONE DEL RISCHIO

TIPOLOGIA	MINACCIA	VULNERABILITÀ	DANNO	CONTROMISURE
Eventi relativi al contesto	Accessi non autorizzati a locali/reparti ad accesso ristretto	Accessi non controllati	Perdita totale o parziale dei dati; accesso o trattamento da parte di soggetti non autorizzati. Asportazione o alterazione delle informazioni.	• Sistema di video sorveglianza. • Badge. • Registro degli accessi.
	Asportazione e furto di strumenti contenenti dati	Accessi non controllati	Perdita totale o parziale dei dati; accesso o trattamento da parte di soggetti non autorizzati. Asportazione o alterazione delle informazioni.	• Sistema di video sorveglianza. • Badge. • Registro degli accessi.

Centro Servizi Ingegneria
Integrated Consulting Services

GESTIONE DEL RISCHIO

TIPOLOGIA	MINACCIA	VULNERABILITÀ	DANNO	CONTROMISURE
Eventi relativi al contesto	Accessi non autorizzati a locali/reparti ad accesso ristretto	Accessi non controllati	Perdita totale o parziale dei dati; accesso o trattamento da parte di soggetti non autorizzati. Asportazione o alterazione delle informazioni.	• Sistema di video sorveglianza. • Badge. • Registro degli accessi.
	Asportazione e furto di strumenti contenenti dati	Accessi non controllati	Perdita totale o parziale dei dati; accesso o trattamento da parte di soggetti non autorizzati. Asportazione o alterazione delle informazioni.	• Sistema di video sorveglianza. • Badge. • Registro degli accessi.

Centro Servizi Ingegneria
Integrated Consulting Services

Rischio Residuo

E' la valutazione del livello di rischio che rimane dopo l'adozione delle misure di sicurezza adottate.

- se il rischio residuo assume livelli considerati accettabili allora il trattamento dei dati può essere effettuato.
- se il rischio residuo risulta «elevato» è necessario approfondire con Valutazione di Impatto (DPIA - Data Protection Impact Assesment).

VALUTAZIONE IMPATTO (DPIA)

Quando è obbligatoria la DPIA ?
(Data Protection Impact Assessment)

(Art. 35) Quando un trattamento "possa presentare un *rischio elevato* per i diritti e le libertà delle persone fisiche". In particolare in caso di:

- una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione;
- trattamento su larga scala di dati sensibili o giudiziari;
- sorveglianza sistematica su larga scala di zone di accesso pubblico;

e per tipologie di trattamenti specificatamente indentificati dal Garante

Centro Servizi Ingegneria
Integrated Consulting Services

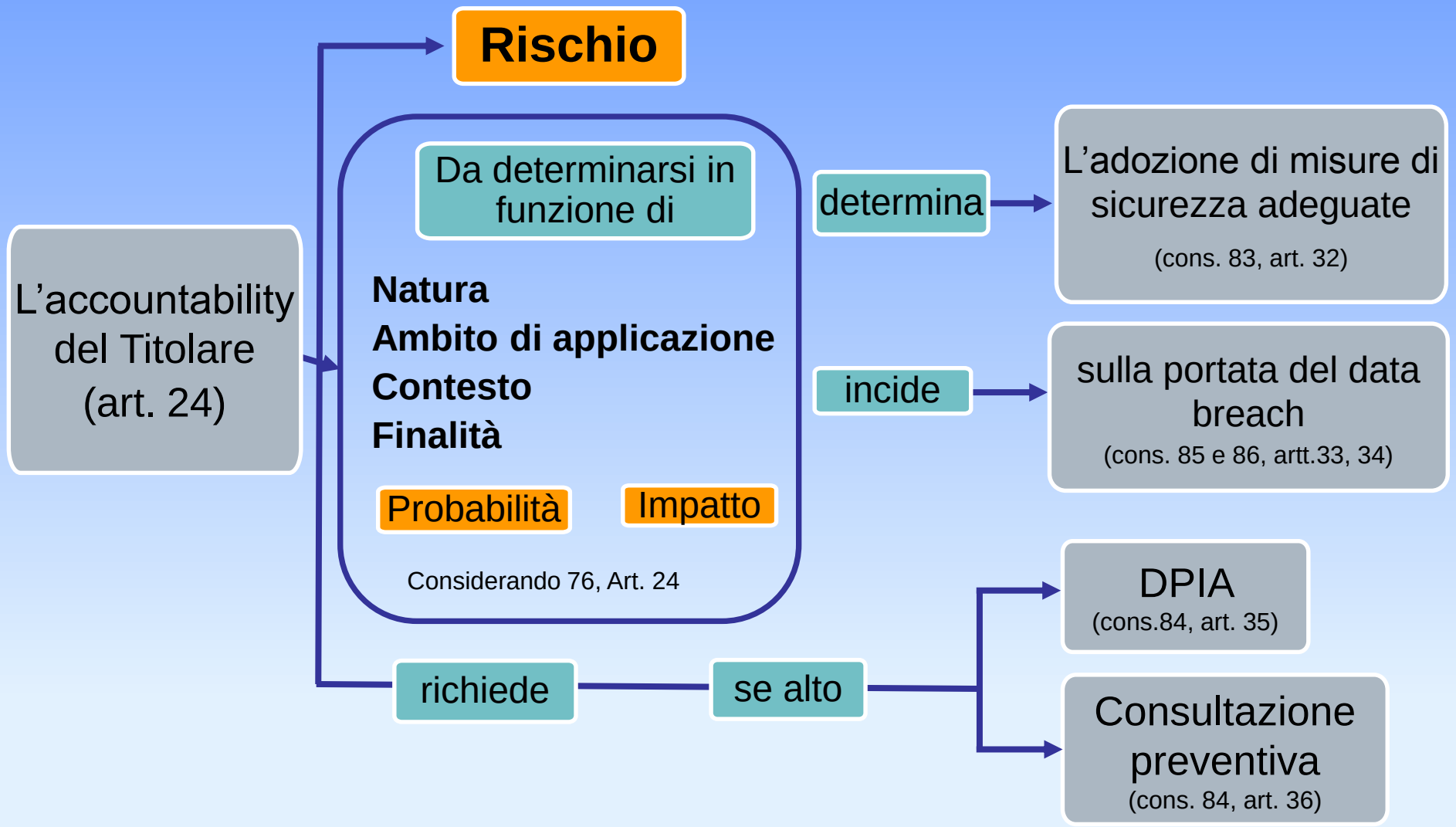
Valutazione d'impatto DPIA e consultazione preventiva

La valutazione d'impatto unitamente all'obbligo di tenuta dei registri sostituisce l'obbligo in generale di effettuare la notificazione all'autorità di controllo e si inserisce nel principio di accountability.

Si riconferma la scelta del regolamento di strategie di tutela sostanziale e non formale.

Se a seguito della valutazione d'impatto permangono rischi elevati il titolare deve richiedere una **verifica preliminare** all'autorità.

Risk based approach



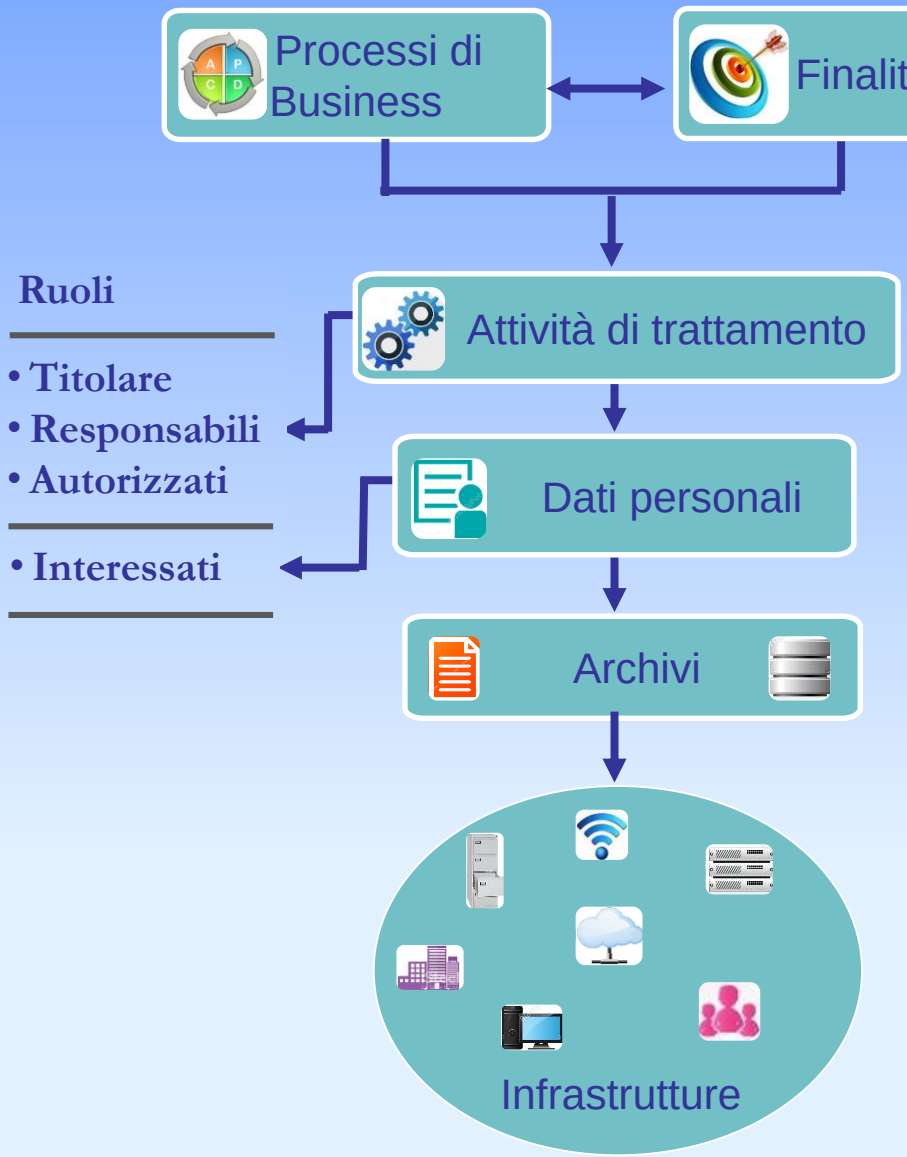
Centro Servizi Ingegneria
Integrated Consulting Services

VALUTAZIONE DEL CONTESTO

Molte prescrizioni del Regolamento presuppongono una **corretta valutazione del contesto** – cioè delle attività di trattamento effettuate - fondata sulla valutazione del rischio effettivo sui diritti e sulle libertà dell'interessato

Centro Servizi Ingegneria
Integrated Consulting Services

VALUTAZIONE DEL CONTESTO:
Processi aziendali - Finalità -Trattamenti



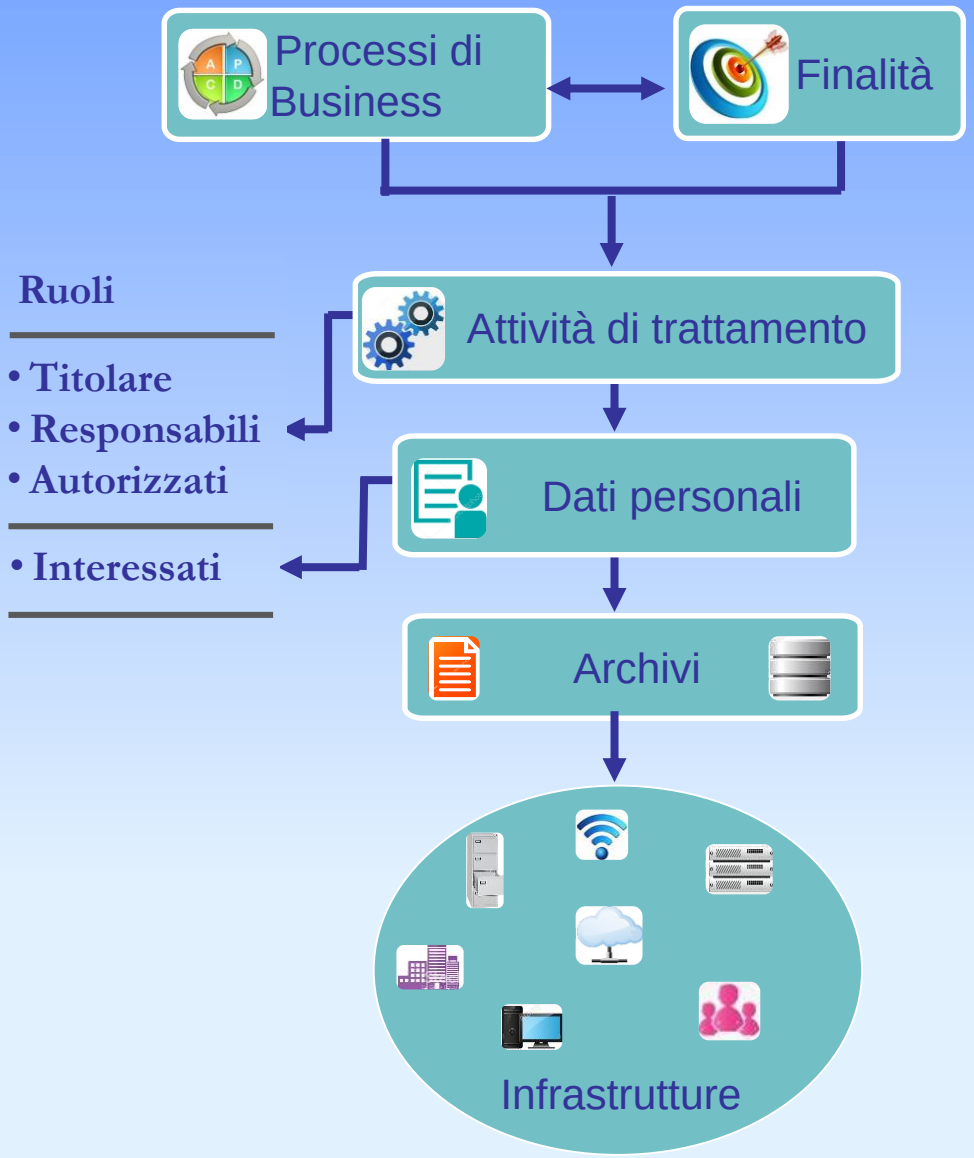
-**Identificazione dei processi** aziendali e delle finalità

-**Identificazione dei trattamenti**:

- quali trattamenti sono svolti nell'ambito di un processo aziendale?
- Chi sono i soggetti coinvolti
- Verifica documentale: nomine e incarichi a responsabili e autorizzati

Centro Servizi Ingegneria
Integrated Consulting Services

VALUTAZIONE DEL CONTESTO: Dati personali

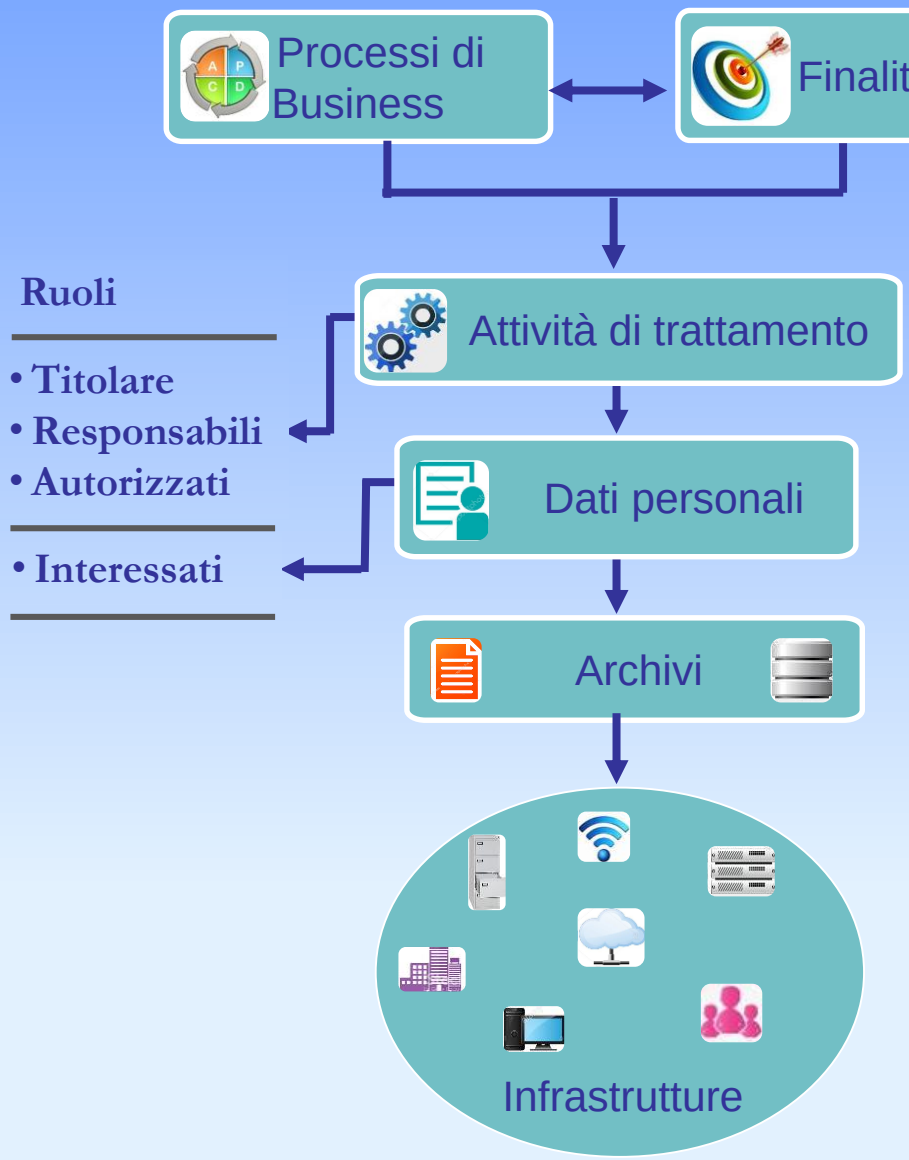


Identificazione dei dati personali:

- Che tipologie di dati personali vengono trattati (anagrafici, di contatto, bancari,ecc.)?
- Sono trattati dati particolari /giudiziari?
- Chi sono gli interessati (dipendenti, fornitori, clienti, ecc.)
- Come sono raccolti i dati ?
- Per quanto tempo sono conservati?
- Verifica documentale: informative e acquisizioni del consenso dagli interessati

Centro Servizi Ingegneria
Integrated Consulting Services

VALUTAZIONE DEL CONTESTO: Infrastruttura



Identificazione degli archivi:

- In che formato sono conservati i dati personali (digitale o analogico)?
- In quali database/archivi/ applicazioni sono elaborati e conservati i dati?

Valutazione dell'infrastruttura:

- Che caratteristiche hanno i database/archivi/applicazioni su cui sono conservati e elaborati i dati?
- Dove si trovano fisicamente?
- Quali soggetti vi possono accedere?
- Quali misure di sicurezza tecniche e organizzative sono applicate all'infrastruttura?

Centro Servizi Ingegneria
Integrated Consulting Services

DOCUMENTARE LA CONFORMITÀ

Il Titolare "deve essere in grado di dimostrare in ogni momento la propria conformità al Regolamento".

Occorre quindi creare e organizzare un apparato documentale che consenta questa **dimostrabilità**, prevedendo delle verifiche e degli aggiornamenti sistematici per essere in grado di dimostrare una protezione costante e dinamica.

Uno strumento utilizzabile a tal fine è rappresentato dal Registro delle attività di trattamento (art. 30).

SISTEMA DI GESTIONE DELLA PRIVACY

Il **TITOLARE** è responsabile per la compliance ai principi privacy e deve essere in grado di DIMOSTRARLA (art. 4, co.2)

Tenuto conto di

NATURA, AMBITO, CONTESTO, FINALITA', RISCHI

Mette in atto

Misure **TECNICHE** ed **ORGANIZZATIVE ADEGUATE** per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR. Dette misure sono **riesaminate** ed **aggiornate** qualora necessario.

Ciò implica l'adozione di un SISTEMA DI GESTIONE DELLA PRIVACY che consenta di gestire nel tempo la compliance.

Centro Servizi Ingegneria
Integrated Consulting Services

SISTEMA DI GESTIONE DELLA PRIVACY

Predisporre un **SISTEMA DI GESTIONE DELLA PRIVACY**

Considerare la privacy sin dalla fase di **progettazione**

Documentare le attività di adeguamento ai singoli obblighi normativi

Attribuire ruoli e responsabilità in materia di privacy coerentemente alle mansioni aziendali (organigramma)

Prevedere regolamenti e procedure per la gestione della privacy

Implementare adeguate politiche di informazione aziendale e meccanismi di controllo per verificare l'applicazione delle misure

Monitorare le misure ed aggiornale se necessario

Centro Servizi Ingegneria
Integrated Consulting Services

SISTEMA DI GESTIONE DELLA PRIVACY

•Dovrà essere predisposta una metodologia di analisi dei rischi ed un processo di privacy by design/default

Dovranno essere individuate adeguate misure da adottare in funzione di tutti i parametri indicati nell'art.32 (es. pseudonimizzazione) e nell'art.25 (es: minimizzazione)

IN PRATICA

•I sistemi dovranno essere predisposti per gestire il periodo di conservazione dei dati, per gestire la richiesta di rettifica, cancellazione o limitazione, dopo il termine stabilito

•Dovranno essere predisposte procedure di verifica periodica delle misure adottate per assicurarne l'efficacia.

Centro Servizi Ingegneria
Integrated Consulting Services

DOCUMENTARE LA CONFORMITÀ

Organizzare le procedure interne in ottica PbD:

- procedure per rendere l'informativa agli interessati
- procedure per la raccolta del consenso
- procedure di risposta all'esercizio dei diritti degli interessati
- procedure di gestione dei data breach
- procedure per integrare la privacy nei prodotti e nei servizi aziendali (minimizzazione dei dati, policy di data retention)
- Procedure di formazione delle persone autorizzate al trattamento
- …

Codici di condotta e certificazioni

Altra novità introdotta dal regolamento: la possibilità di dimostrare il rispetto degli obblighi, la validità delle procedure e la solidità delle regole attraverso strumenti di "soft law" la cui adesione è volontaria: **codici di condotta, meccanismi di certificazione, marchi di protezione dei dati.**

Sono intesi come mezzo per dimostrare l'affidabilità e la conformità del sistema privacy ai requisiti richiesti: privacy by design e by default, sicurezza del trattamento, valutazione d'impatto, qualità ed esattezza dei dati

Certificazioni e adesione a codici di condotta approvati non manlevano da responsabilità, ma forniscono un valido strumento di accountability

LA SICUREZZA INFORMATICA

Considerato che una buona parte degli strumenti utilizzati per il trattamento dei dati personali sono di carattere tecnologico/informatico la norma ISO 27001 diventa un'importante base per l'approccio al sistema privacy.

Lo standard definisce i requisiti per l'implementazione di un Sistema di Gestione della Sicurezza delle informazioni includendo aspetti relativi alla sicurezza logica, fisica ed organizzativa.

La norma ISO 27001 è finalizzata alla standardizzazione delle modalità adatte a proteggere i dati e le informazioni da minacce di ogni tipo, al fine di assicurarne l'integrità, la riservatezza e la disponibilità.

Centro Servizi Ingegneria
Integrated Consulting Services

INTERAZIONE MULTIDISCIPLINARE

La compliance al GDPR è l'insieme di numerosi adempimenti, solo una parte dei quali riferibili all'area Sistemi informativi di un'azienda, e perciò richiede l'interazione multidisciplinare tra legali, tecnici e responsabili organizzativi, per la definizione di procedure calate nei processi, nei ruoli, nelle dinamiche interne ed esterne delle singole realtà aziendali.

CATENA DELLA SICUREZZA

La policy aziendale sulla sicurezza dei dati sarà veramente efficace se – oltre a contenere una serie di prescrizioni e raccomandazioni tagliate su misura della organizzazione aziendale – verrà **veicolata tra i dipendenti** ed i soggetti terzi che trattano i dati ed utilizzano la strumentazione informatica dell'azienda, in modo da renderli pienamente consapevoli dei rischi legati al trattamento dei dati personali.

Ciò perché nella "catena della sicurezza" spesso l'anello debole è rappresentato dall'elemento umano!

Centro Servizi Ingegneria
Integrated Consulting Services

Centro Servizi Ingegneria

Integrated Consulting Services

20th Anniversary 1994 • 2014

GRAZIE PER L'ATTENZIONE!

Dott.sa Laura Pellegrino

Email: laura.pellegrino@csisrl.com