

Corso Privacy generale

Avv. Aurora Cavo (DPOffice Regione Toscana – Consorzio Metis)

❑ **Prima Parte**

Principi, nozioni fondamentali, procedure *data protection: finalità e base giuridica del trattamento dei dati personali in ambito pubblico, l'individuazione dei ruoli nel trattamento dei dati personali, data breach, diritti degli interessati, provvedimenti sanzionatori*

❑ **Seconda Parte – Data Protection Policy regionale**

1. Il Processo Data Protection by Design e by Default
2. Il Processo per le garanzie e le tutele dei diritti degli interessati
3. Il Processo di gestione degli incidenti

- ❑ **GDPR: *General Data Protection Regulation***
(regolamento generale sulla protezione dei dati).
Regolamento UE 2016/679 entrato in vigore il 25 maggio 2016, con efficacia a partire dal 25 maggio 2018 in tutti gli Stati membri dell'UE.

- ❑ **Codice della Privacy (d.lgs. n. 196/2003)**
Modificato dal d.lgs. n. 101/2018, per adeguare la disciplina della protezione dei dati personali al GDPR.

Art. 4 GDPR

1) **Dato personale:** Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale

- **Dati anagrafici** (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale, altro...)
- **Dati di contatto** (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)
- **Dati di accesso e di identificazione** (username, password)
- **Dati di pagamento** (numero di conto corrente, dettagli della carta di credito...)
- **Dati relativi alla fornitura di un servizio di comunicazione elettronica** (dati di traffico, dati relativi alla navigazione internet...)
- **Dati relativi a documenti di identificazione/riconoscimento** (carta di identità, passaporto, patente, CNS, altro...)
- **Dati di localizzazione**



Art. 4 GDPR

2) **Trattamento:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Alcune operazioni di trattamento

Raccolta (presso l'interessato o presso terzi)

Utilizzo (uso del dato, es. telefonata; invio di una email...)

Consultazione (es. accesso in lettura)

Modifica

Comunicazione

Diffusione

Estrazione

Cancellazione

Conservazione

Registrazione

Distruzione

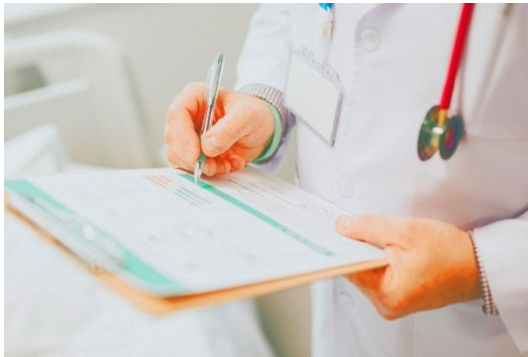


Art. 9, par. 1, GDPR

Categorie particolari di dati personali

È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Alcune tipologie di dati personali «particolari»



Adesioni a partiti politici

Iscrizioni a sindacati

Appartenenza a categorie protette

Aderenza a una confessione religiosa

Informazioni sul proprio stato di salute

Art. 10 GDPR

Dati giudiziari (o dati relativi a condanne penali e reati)

L'art. 10 dispone che il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.

Art. 5, 24 e 25 GDPR

- Liceità, correttezza e trasparenza;
- Limitazione delle finalità;
- Minimizzazione;
- Esattezza;
- Limitazione della conservazione;
- Integrità e riservatezza dei dati;
- Accountability;
- *Privacy by design e privacy by default*

Art. 5, par. 1 lett. a):

I dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.

Art. 5, par. 1 lett. b):

I dati personali sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità...

Art. 5, par. 1 lett. c):

I dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

Art. 5, par. 1 lett. d):

I dati personali sono esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.

Art. 5, par. 1 lett. e):

I dati personali sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.

Art. 5, par. 1 lett. f):

I dati personali sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

Art. 5, par. 2, GDPR:

«Il titolare del trattamento è competente per il rispetto del paragrafo 1 e **in grado di provarlo.**»

Ciascuna organizzazione che tratta dati personali deve mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere **in grado di dimostrare**, che il trattamento dei dati personali è effettuato conformemente al Regolamento.



Privacy by design & Privacy by default

Privacy by design

La protezione dei dati deve essere integrata dalla primissima fase di progettazione delle operazioni di trattamento fino alla loro ultima distribuzione, all'utilizzo e all'eliminazione finale.

L'obiettivo primario è il rispetto dei diritti degli interessati, assicurando che la protezione dei dati sia garantita all'atto della progettazione iniziale dei sistemi di trattamento e nei successivi funzionamenti o sviluppi.

Privacy by default

I trattamenti devono rispettare, per impostazione predefinita, i principi generali della protezione dei dati, sempre con particolare riferimento al principio di minimizzazione dei dati e di limitazione delle finalità.

Occorre mettere in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità.

Privacy by design & Privacy by default

Esempio: progettazione di un sito o servizio digitale



L'organizzazione sta progettando lo sviluppo di un sito o di un servizio/applicazione digitale.

Occorre che la politica sulla privacy:

- non contenga una quantità eccessiva di informazioni di difficile comprensione per l'interessato medio, e che sia scritta in un linguaggio chiaro e conciso e possa consentire all'utente di comprendere le modalità di trattamento dei suoi dati personali

- non deve essere di difficile accesso per gli interessati. Pertanto, deve essere messa a disposizione e visibile su tutte le pagine del sito, o prima di accedere al servizio in questione.



L'acquisizione di dati personali da parte di un'autorità pubblica deve essere previsto da disposizioni giuridiche: l'interesse del soggetto pubblico al trattamento di dati personali discende direttamente dalla norma attributiva del potere.

L'amministrazione può trattare quindi dati personali in vista della finalità posta dalla norma che le attribuisce il potere di raccogliere gli stessi. In relazione ai soggetti pubblici, la finalità del trattamento è predeterminata dalle norme che attribuiscono agli stessi funzioni e competenze.

Esempi

Trattamento dei dati personali di soggetti richiedenti contributi sulla base della normativa di settore; trattamento dei dati personali necessari all'espletamento delle procedure d'appalto e ai relativi controlli; accesso agli atti...

Il principio di liceità: le basi giuridiche del trattamento dei dati personali comuni (Art. 6, GDPR)



1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

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)

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)

Art. 6, lett. 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



Il trattamento deve essere effettuato in conformità a un obbligo di legge al quale l'autorità pubblica è soggetta, basato sul diritto nazionale o europeo.

Il GDPR non impone che ci sia un atto normativo specifico per ogni singolo trattamento, tuttavia l'art. 2-ter del Codice Privacy («Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri») prevede che:

*«La base giuridica prevista dall'articolo 6, paragrafo 3, lettera b), del regolamento è costituita esclusivamente da **una norma di legge o di regolamento o da atti amministrativi generali**».*

Come principio di carattere generale viene sancito il divieto di trattamento dei dati particolari, ma tale divieto non si applica quando ricorrono determinati casi previsti dalla disposizione.

Per esempio, è possibile trattare dati «particolari» quando:

- L'interessato ha prestato il proprio consenso;
- Per far valere un diritto in giudizio;
- Per motivi di **interesse pubblico rilevante** sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e misure appropriate e specifiche per tutelare l'interessato
- Per finalità di medicina e di salute, interesse pubblico nel settore della sanità pubblica
- **Archiviazione nel pubblico interesse, ricerca scientifica o a fini statistici...**

1. I trattamenti delle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del Regolamento, necessari per **motivi di interesse pubblico rilevante** ai sensi del paragrafo 2, lettera g), del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di **legge o di regolamento o da atti amministrativi generali** che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Regolamento 26 ottobre 2021, n. 37/R - Preambolo

La l.r. 13/2006 , adeguata dalla legge regionale 6 luglio 2020, n. 51 (Legge di manutenzione dell'ordinamento regionale 2019), all'articolo 1 prevede che **il trattamento delle categorie particolari di dati personali e dei dati personali relativi a condanne penali e ai reati da parte della Giunta regionale, delle aziende sanitarie, degli enti, aziende e agenzie regionali, nonché degli altri soggetti pubblici nei confronti dei quali la Regione esercita poteri di indirizzo e controllo** è disciplinato con regolamento regionale nel rispetto dei principi del Regolamento (UE) 2016/679 e del novellato d.lgs. 196/2003

Il regolamento identifica:

- i tipi di dati che possono essere trattati
- le operazioni eseguibili
- il motivo di interesse pubblico rilevante
- le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato

con riferimento ai trattamenti delle categorie particolari di dati personali e dei dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza effettuati per il perseguimento delle rilevanti finalità di interesse pubblico individuate da espressa disposizione normativa, ove non siano legislativamente specificati i tipi di dati e le operazioni eseguibili.

- *Elenco dei trattamenti di competenza della Regione Toscana-Giunta regionale, degli enti, aziende e agenzie regionali, degli enti controllati e vigilati dalla Regione Toscana*

Le **schede** individuano i trattamenti di competenza della Giunta con i tipi di dati che possono essere trattati, le operazioni eseguibili su tali dati, il motivo di interesse pubblico rilevante e le misure appropriate e specifiche, tra cui:

1. Instaurazione e gestione del rapporto di lavoro del personale
2. Attività ispettiva
3. Attività di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria
4.

Nelle situazioni in cui emergono gravi rischi per la protezione dei dati (es. profilazione), serve un **consenso esplicito**. **Tuttavia, nel settore pubblico**



*«...è improbabile che le **autorità pubbliche** possano basarsi sul consenso per effettuare il trattamento, poiché ...sussiste spesso un **evidente squilibrio di potere** nella relazione tra il titolare del trattamento e l'interessato. In molti di questi casi è inoltre evidente che l'interessato non dispone di alternative realistiche all'accettazione (dei termini) del trattamento. Il Gruppo di lavoro ritiene che esistano altre basi legittime, in linea di principio più appropriate, per il trattamento da parte delle autorità pubbliche»*

ossia

Articolo 6, par. 1 **lettera c) e lettera e), GDPR**

L'art. 13 prevede che in caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:

- a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
- b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;
- c) le **finalità del trattamento** cui sono destinati i dati personali nonché la **base giuridica del trattamento**;
- d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
- e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione...

Chi è? Persona fisica o giuridica che determina le finalità e i mezzi del trattamento di dati personali.

Quali poteri?

- determina le finalità e i mezzi del trattamento
- decide i soggetti subordinati, all'interno della propria struttura (dipendenti) o all'esterno a cui delegare le operazioni di trattamento

Giunta Regionale: Titolare dei trattamenti afferenti alle finalità dell'ente Regione Toscana

Direttore Generale, Avvocato Generale, Direttori: assumono a seguito della delibera 585/2018 le figure di Delegati del Titolare per i trattamenti di loro diretta responsabilità e assolvono, nelle forme più opportune, all'attuazione dell'organizzazione e dei processi in materia data protection

Dirigenti: assumono, a seguito della delibera 585/2018, la figura di Delegato del Titolare per i trattamenti di loro diretta responsabilità.

Quali obblighi? 3 categorie

1) In materia di sicurezza

- predisposizione delle misure tecniche e organizzative adeguate (inclusa verifica e aggiornamento periodico)
- designazione di un DPO, se necessario e i soggetti responsabili del trattamento, interni o esterni, istruendoli adeguatamente
- messa in atto tempestiva di ogni contromisura necessaria di caso di *data breach*
- tenuta del **registro** dei trattamenti

IL REGISTRO DEI TRATTAMENTI

Cosa è? Strumento che consente al titolare del trattamento e all'autorità di controllo, su richiesta, di disporre di un quadro complessivo dei trattamenti di dati personali svolti dallo specifico soggetto.

Sorta di «giornale di bordo» che deve essere costantemente **aggiornato**.

Come si redige? Si può redigere tramite software, basta che abbia i contenuti previsti dal Regolamento.

- a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del DPO;
- b) le finalità del trattamento;
- c) una descrizione delle categorie di interessati e delle categorie di dati personali;
- d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi (extra UE)
- e) ove applicabile, i trasferimenti di dati personali verso un paese terzo;
- f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate

ALTRI OBBLIGHI DEL TITOLARE

2) Obblighi nei confronti degli interessati:

- fornire all'interessato l'informativa sul trattamento dei dati personali
- dotarsi di un'organizzazione adeguata ed efficiente al fine di provvedere alle istanze presentate dall'interessato

3) Obblighi di collaborazione con le autorità di controllo:

- collaborare con l'Autorità Garante, come nel caso della notifica di violazione alle misure di sicurezza; con gli organismi indipendenti di certificazione e con il DPO

Chi sono? Due o più titolari del trattamento che determinano congiuntamente le finalità e i mezzi del trattamento

Necessità di un **accordo interno** fra contitolari.

Solidarietà tra i contitolari.

Chi è? Persona fisica o giuridica, autorità pubblica o altro organismo che tratta i dati personali per conto del titolare del trattamento.

Quale designazione? Nominato dal titolare **con contratto** (o altro atto giuridico). **Quale forma del contratto?** Forma scritta, anche in formato elettronico.

Quali contenuti obbligatori del contratto?

- oggetto e durata del trattamento;
- doveri e compiti del responsabile del trattamento;
- ambito di rischi e finalità del trattamento;
- natura e finalità del trattamento;
- modalità di svolgimento delle attività di trattamento;
- tipo di dati personali trattati;
- categorie di persone fisiche coinvolte;
- obblighi e diritti del titolare del trattamento.

OBBLIGHI DEL RESPONSABILE

- Prestare garanzie sufficienti di attuare **misure tecniche e organizzative** adeguate
- Effettuare il trattamento attenendosi alle condizioni stabilite e alle **istruzioni impartite dal titolare** (verifiche periodiche)
- Mettere in atto le **misure di sicurezza**
- Assistere il titolare nel momento della **valutazione di impatto**
- Collaborare con il **DPO**
- Collaborare con il titolare affinché quest'ultimo possa adempiere agli **obblighi di notifica** nei confronti delle Autorità di controllo e dell'interessato
- **Cancellare o restituire i dati** personali al termine della prestazione del servizio, su decisione del titolare del trattamento.

Il Responsabile può nominare un sub-responsabile qualora vi ricorra per l'esecuzione di specifiche attività di trattamento per conto del titolare.

Quale designazione? In **forma scritta attraverso contratto di nomina (o qualunque altro atto giuridico valido) previa autorizzazione del titolare.**

In caso di nomina di un sub-responsabile, il responsabile dovrà informare il titolare il quale potrà **autorizzare la nomina, oppure opporsi.**

Designazione del sub-responsabile attraverso **autorizzazione generica oppure specifica.**

Con la prima il Titolare autorizza il Responsabile ad avvalersi di un sub responsabile non ancora individuato.

Quali obblighi? Stessi obblighi del responsabile.

INCARICATO («Autorizzato»)

Chi è? Chi **effettua materialmente le operazioni di trattamento** sui dati personali, mero esecutore di compiti. Chiunque agisca sotto l'autorità del titolare del trattamento non può trattare i dati se non è stato previamente autorizzato dallo stesso.

Quale designazione? Nomina per iscritto e che individui puntualmente l'ambito del trattamento consentito.

INCARICATO («Autorizzato»)

- ✓ Con la DGR 585/2018 i dipendenti assegnati alle strutture dei dirigenti delegati e i soggetti che vi operano ad altro titolo, che agiscono sotto la loro autorità, sono stati autorizzati al trattamento dei dati personali, stabilendo che l'ambito di operatività di ciascun autorizzato (tipi di dati personali trattati, operazioni di trattamento eseguibili, banche dati/archivi acceduti...) deve essere appositamente censito nella procedura informatizzata "Registro trattamenti – Trattamenti Dati Personali" a cura del dirigente delegato. Tale censimento integra e completa l'autorizzazione del titolare e legittima le persone autorizzate al trattamento dei dati personali.
- ✓ Istruzioni generali per le persone autorizzate al trattamento dei dati personali: Disciplinare – Addendum DPP

Chi è? Figura implicitamente prevista dal GDPR, laddove mette in capo al Titolare responsabilità e attività che prefigurano competenze tecniche specialistiche in materia di *data protection*, non riconducibili direttamente alle competenze richieste per svolgere il ruolo di Titolare. Esempio:

- individuazione delle basi giuridiche dei trattamenti
- la determinazione della misura dei rischi di natura tecnica ed organizzativa...

E' una figura competente in grado di supportare la struttura nei rapporti con altre strutture, interne o esterne all'organizzazione, referenti per le specifiche competenze.

Quali compiti?

- **sorvegliare sull'osservanza del Regolamento:**

Raccolta di informazioni per individuare i trattamenti svolti; analisi e verifica dei trattamenti in termini di loro conformità, attività di informazione, consulenza e indirizzo nei confronti di titolare o responsabile.

- operare con l'Autorità di controllo e con l'interessato come **punto di contatto**.

Quali competenze? Giuridiche, aziendali, informatiche.

Deve essere facilmente **raggiungibile** dall'interessato.
Non deve essere in **conflitto di interessi**.

Chi può essere nominato DPO?

- la funzione di DPO può essere esercitata in base a **un contratto di servizi** stipulato con una persona fisica o giuridica esterna all'azienda titolare/responsabile del trattamento.

Quali attività? Il titolare del trattamento e il responsabile del trattamento assicurano che **il DPO sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.**

Ciò significa garantire, per esempio:

1. la presenza del DPO ogniqualvolta debbano essere assunte decisioni che impattano sulla protezione dei dati;
2. che il parere del DPO riceva sempre la dovuta considerazione;
3. che il DPO sia consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

DATA BREACH

L'art. 33 del Regolamento dispone che in caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente senza ingiustificato ritardo, ove possibile **entro 72 ore** dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Il mancato o ritardato adempimento della comunicazione espone alla possibilità di **sanzioni amministrative**.



"la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati"

Tipi di violazioni di dati personali:

"violazione della riservatezza", in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;

"violazione dell'integrità", in caso di modifica non autorizzata o accidentale dei dati personali;

"violazione della disponibilità", in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.



I DIRITTI DELL'INTERESSATO

A chi spettano e verso chi? Il regolamento attribuisce specifici diritti all'interessato, il quale, per l'esercizio di tali diritti, può rivolgersi direttamente al titolare del trattamento.

Quali diritti?

1. DIRITTO DI INFORMAZIONE: diritto a ricevere una corretta informazione in **relazione ai dati raccolti e trattati, alle finalità del trattamento, alla base giuridica del trattamento e ai diritti che gli sono attribuiti, nonché le modalità per esercitarli.** Tutto ciò avviene a mezzo dell'**informativa** rivolta all'interessato.

Quali termini? Termine per la risposta all'interessato: **1 mese, estensibile fino a 3 mesi in casi di particolare complessità;** salvo in ogni caso il **riscontro** all'interessato in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità.

Quali costi? Esercizio dei diritti **gratuito** per l'interessato, ma se le richieste dell'interessato sono **manifestamente infondate o eccessive,** il titolare del trattamento può addebitare un contributo spese ragionevole.

2. ACCESSO: diritto di ottenere dal titolare del trattamento la **conferma che sia o meno in corso un trattamento**, e in tal caso, di ottenere l'accesso ai dati personali e ad una serie di informazioni, fra cui le finalità del trattamento, le categorie di dati e il periodo di conservazione previsto.

3. RETTIFICA: diritto di ottenere dal titolare del trattamento la **rettifica dei dati personali inesatti** che lo riguardano senza ingiustificato ritardo, diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

4. OBLIO: diritto dell'interessato di ottenere la **cancellazione** dei dati personali che la riguardano se la conservazione di tali dati viola il regolamento o il diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento.

5. LIMITAZIONE DEL TRATTAMENTO: diritto più esteso rispetto al “blocco” del trattamento di cui Codice privacy, esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), ma anche se l’interessato chiede la rettifica dei dati (in attesa di tale rettifica da parte del titolare) o si oppone al loro trattamento (in attesa della valutazione da parte del titolare).

Fra le modalità per limitare il trattamento dei dati personali : **il trasferire temporaneamente i dati selezionati verso un altro sistema di trattamento, il rendere i dati personali selezionati inaccessibili agli utenti o il rimuovere temporaneamente i dati pubblicati da un sito web.**

6. PORTABILITÀ DEI DATI: diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali che lo riguardano forniti ad un titolare del trattamento, e il diritto **di trasmettere tali dati a un altro titolare del trattamento** senza impedimenti da parte del titolare precedente. Ciò implica che il titolare trasferisca direttamente i dati portabili all'altro titolare indicato dall'interessato, se tecnicamente possibile.

Per quali trattamenti e per quali dati? Solo per i trattamenti automatizzati; sono portabili **solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato.**

7. OPPOSIZIONE: diritto dell'interessato di **opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano.**

Il titolare del trattamento si deve astenere dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi per continuare il trattamento che prevalgono sui diritti dell'interessato, oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Provvedimenti sanzionatori dell'Autorità Garante per la protezione dei dati personali



L'art. 83 del Regolamento prevede che la violazione di determinate disposizioni è soggetta a sanzioni amministrative pecuniarie fino a 20.000.000 EUR, o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

La violazione di altre disposizioni è soggetta a sanzioni amministrative pecuniarie fino a 10.000.000 EUR, o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.



Ordinanza di ingiunzione del 15 settembre 2022 - Regione Lazio

Reclamo di una donna che aveva ricevuto dalla ASL di Rieti un invito a partecipare al programma di screening del tumore del collo dell'utero rivolto alla figlia deceduta nel 1995.

Le campagne di screening venivano svolte dalle ASL utilizzando una piattaforma regionale. Il Garante ha contestato alla Regione il mancato rispetto dei principi di esattezza e correttezza dei dati trattati e la non corretta individuazione dei ruoli ricoperti dai soggetti coinvolti. Inoltre:



Non corretta individuazione di un'idonea base giuridica del trattamento



Inidoneità dei contenuti dell'informativa sul trattamento dei dati personali



Sanzione: € 100.000

Provvedimento del 28 aprile 2022 – INAIL

INAIL ha notificato al Garante tre data breach verificatesi tra il 2019 e il 2020 riguardanti il servizio online «Sportello Virtuale Lavoratori», che consente ai cittadini vittime di infortunio sul lavoro o malattia professionale di visualizzare lo stato delle proprie pratiche presso INAIL. Alcuni utenti hanno avuto la possibilità di visualizzare dati personali, anche relativi alla salute, di altri interessati utenti del servizio.



Mancata adozione delle misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi presentati dal trattamento



Sanzione: € 50.000

Provvedimento del Garante alla Regione Lazio – provv. n. 196 del 21 marzo 2024

Un data breach -causato da un ransomware introdotto nel sistema attraverso un portatile in uso a un dipendente della Regione- ha bloccato l'accesso a molti servizi sanitari impedendo, tra l'altro, la gestione delle prenotazioni, i pagamenti, il ritiro dei referti, la registrazione delle vaccinazioni.

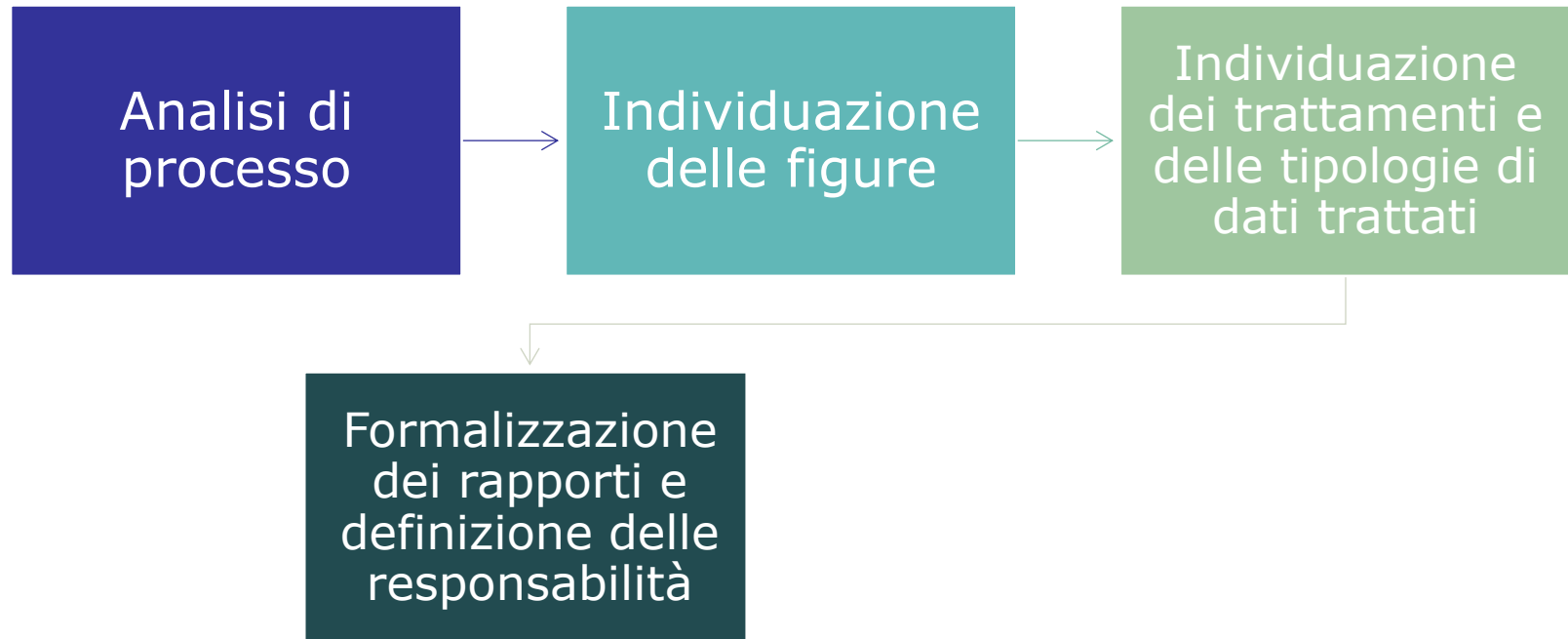


Adozione di sistemi non aggiornati e mancata adozione di misure di sicurezza adeguate a rilevare tempestivamente le violazioni di dati personali e a garantire la sicurezza delle reti informatiche



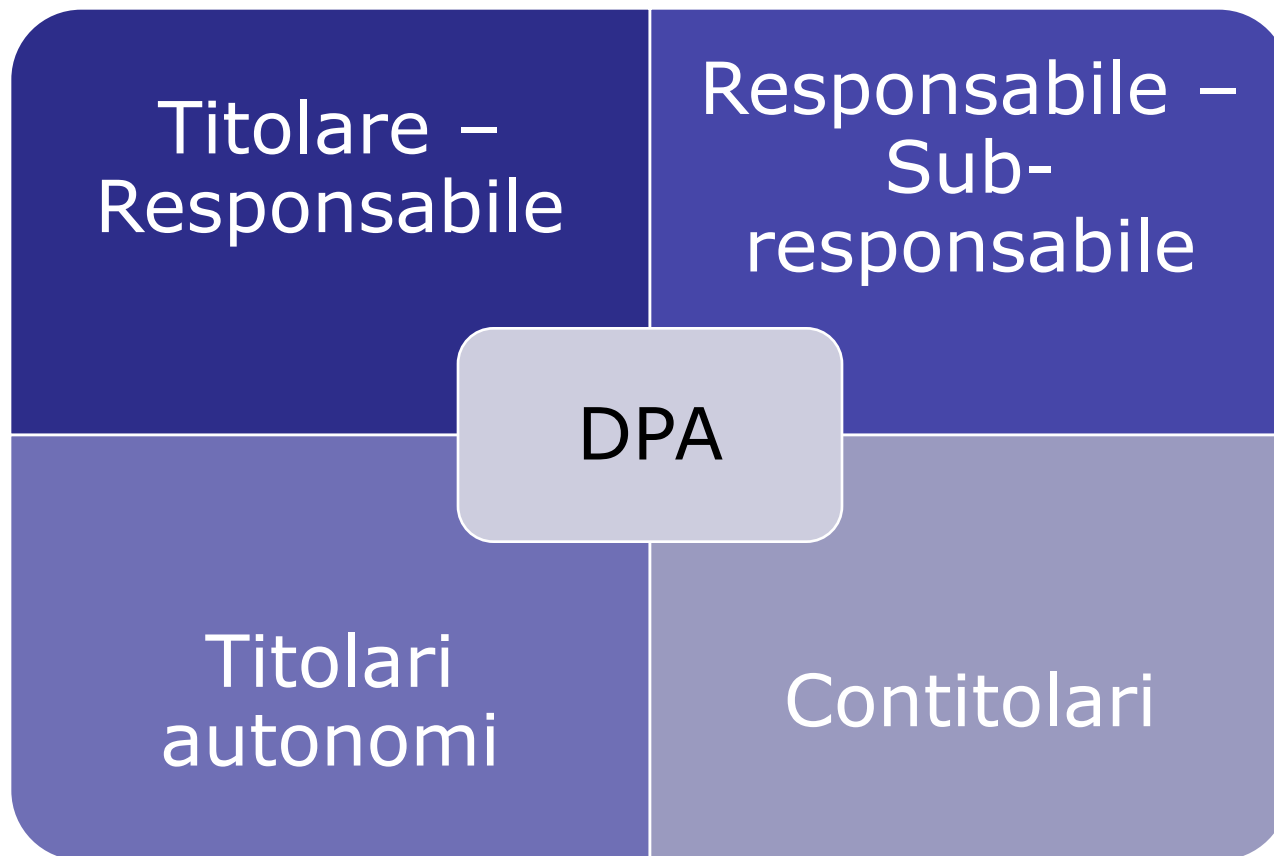
Sanzione: € 120.000

Il Processo Data Protection by Design e by Default



L'individuazione dei ruoli può avvenire sulla base di una norma di riferimento, o su base fattuale, e i ruoli devono essere formalizzati: il **Data Protection Agreement (DPA)** può essere un **accordo separato** fra le parti o un **articolato specifico** inserito all'interno di contratti, convenzioni, protocolli d'intesa che regoli le rispettive responsabilità in ambito data protection. Tramite il DPA possono essere regolati i rapporti fra....

Il Processo Data Protection by Design e by Default



Il Processo per le garanzie e le tutele dei diritti degli interessati

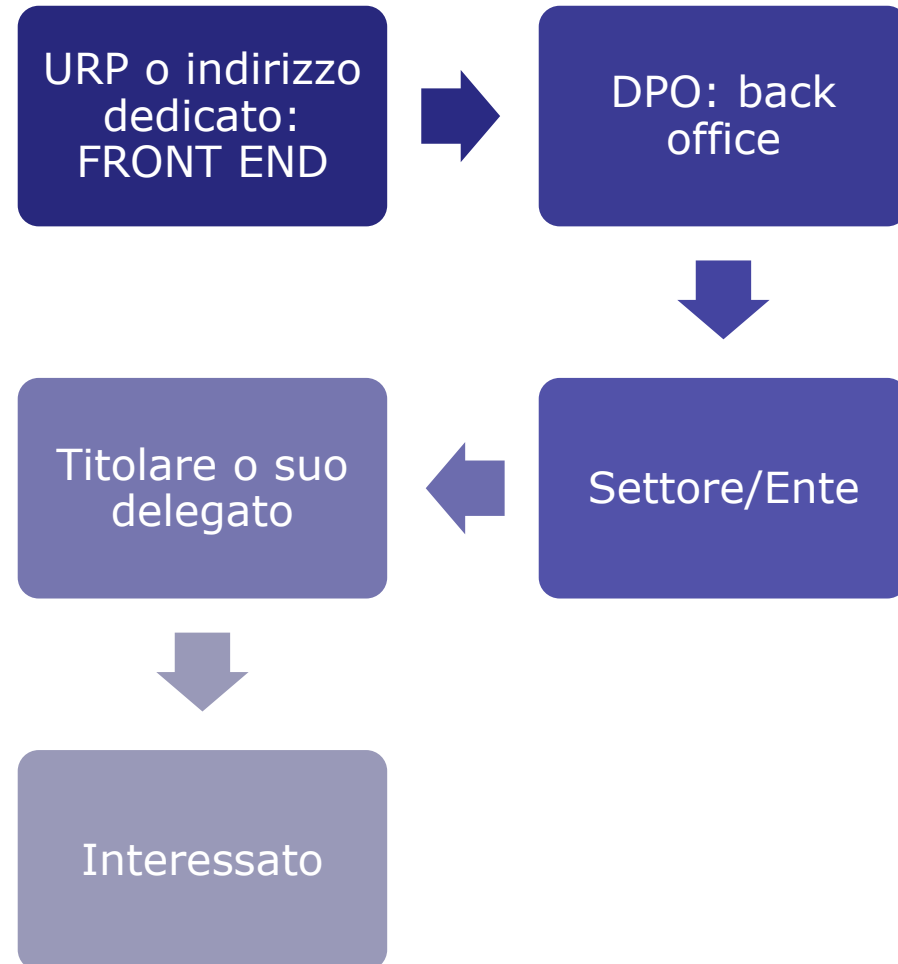


Il DPO riceve la richiesta dall'URP (o indirizzo email appositamente dedicato del Titolare) e la SMISTA al Settore/Ente cui attiene il trattamento in questione, per acquisire ogni informazione utile. La risposta all'interessato deve essere elaborata dal Settore/Ente, con il supporto del DPO, e deve essere data sullo stesso canale e con gli stessi mezzi con i quali è stata formulata la richiesta e firmata dal Titolare o suo delegato.

Qualora il DPO verifichi la impossibilità o la non applicabilità di una risposta ne informa il Titolare che decide se applicare la deroga alla risposta.

Tali casi sono:

- a. impossibilità di identificare l'interessato;
- b. carattere manifestamente infondato o eccessivo della richiesta inviata da parte dell'interessato, in particolare per via del carattere ripetitivo della stessa.



Il Processo di gestione degli incidenti

Chiunque venga a conoscenza di violazioni di dati personali, contatta il DPO e/o il Security Manager (attualmente, il CISO)

Il Security Manager (CISO) prende in carico la segnalazione dell'incidente e provvede alla registrazione nel Registro degli Incidenti

Il Titolare o suo delegato, avvalendosi anche del supporto del CISO e del DPO, deve valutare se l'incidente può comportare un rischio per i diritti e le libertà delle persone fisiche

Il Processo di gestione degli incidenti

...ovvero se
l'incidente può
cagionare:
discriminazioni;
furto d'identità;
perdite finanziarie;
qualsiasi altro
danno economico o
sociale significativo

Se il Titolare o suo
delegato ritiene
che l'incidente
rappresenti un
rischio per i diritti
e le libertà delle
persone fisiche,
procede alla
notifica all'Autorità
Garante

La procedura di
notifica, attraverso
il sito istituzionale
dell'Autorità, deve
essere completata
entro 72 ore dal
momento in cui si
è venuti a
conoscenza
dell'incidente

Cybersecurity: insieme di tecnologie, programmi, processi e tecniche concepiti e messi in atto per proteggere dispositivi, dati e reti informatiche



sicurezza del contenitore informatico

Data Protection: sicurezza delle informazioni contenute all'interno.



RISCHIO CYBER VS. RISCHIO GDPR

- ❑ Il rischio individuato dal **GDPR** afferisce alla distruzione, alla perdita, alla modifica, alla modificazione, alla divulgazione non autorizzata o all'accesso ai dati personali trasmessi, conservati o comunque trattati. Il rischio riguarda quindi la **disponibilità** dei dati, l'**integrità** dei dati e la loro **riservatezza**.
- ❑ Il rischio **cybersecurity** è correlato all'eventualità che si verifichi l'interruzione del servizio oggetto di incidente e alla capacità del sistema di superare le conseguenze dell'incidente stesso senza che questo pregiudichi la prestazione del servizio.



Un **incidente di sicurezza** è un evento (o una serie di eventi) di origine dolosa o accidentale, esterno o interno all'organizzazione, che può comportare la compromissione dei dati detenuti, mettendo a rischio uno o più dei tre principi della sicurezza delle informazioni: riservatezza, integrità e disponibilità.

Un **data breach** è una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

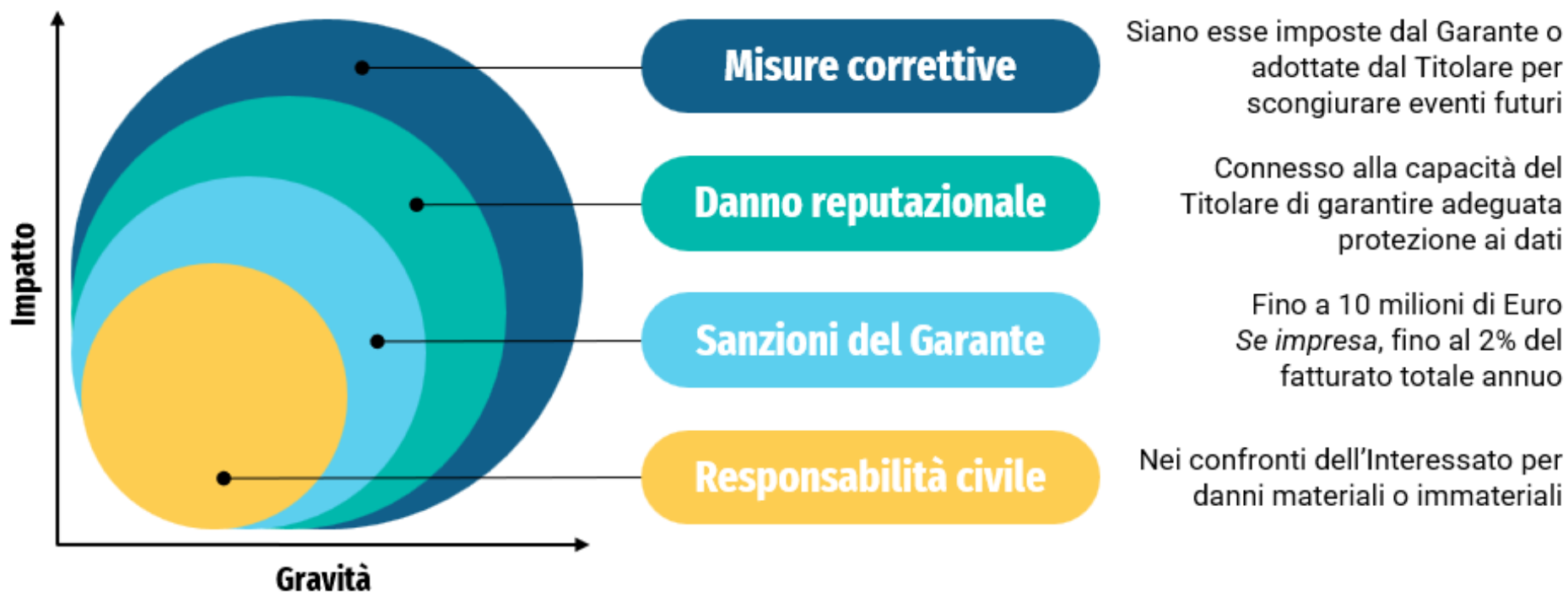
Non tutte le violazioni informatiche comportano un data breach, e non tutti i data breach comportano necessariamente una violazione informatica.

COSA FARE IN CASO DI DATA BREACH?

Le 6 regole da seguire



Le conseguenze di un *data breach*



RANSOMWARE

Ransom(riscatto) Software



RANSOMWARE: LE P.A. SOTTO ATTACCO

- Regione Lazio (2021) – Ransomware con blocco dei servizi per oltre un mese, tra cui il sistema sanitario online (CUP, prestazioni specialistiche..). Perdita di disponibilità dei dati personali accertata
- Regione Basilicata (2024) – Ransomware con attacco al sistema sanitario e richiesta di riscatto



Social Engineering

L'anello debole di qualsiasi catena di sicurezza è l'essere umano.

Il **social engineering** cerca di sfruttare tale anello debole sfruttando la curiosità, l'altruismo, il rispetto, la vanità o il timore nei confronti dell'autorità, al fine di spingere le persone a rivelare determinate informazioni o consentire l'accesso a un sistema informatico.

Phishing

Indurre la persona a condividere info sensibili



Scareware

Offrire una soluzione per infettare un dispositivo



Baiting

Offrire qualcosa per far scaricare un file dannoso



Pretexting

Impersonare qualcuno per ottenere dati



Da avast.com

PHISHING

Deriva dall'inglese *fishing*, pescare.
Lo scopo è carpire info riservate e sensibili.

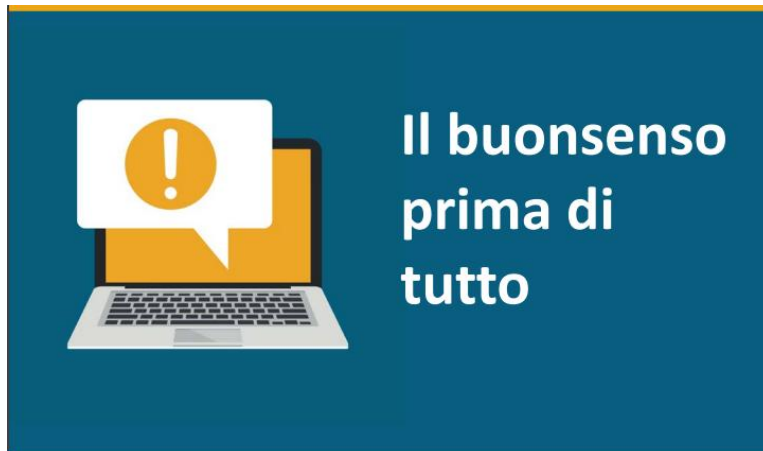
Viene messo in atto tramite un'email che sembra a tutti gli effetti provenire da un soggetto conosciuto o conoscibile.

Il messaggio avvisa della scadenza di una password, di un rinnovo di una carta di credito, di un conto corrente bloccato, prospetta occasioni di lavoro, etc.

La persona viene indirizzata tramite link ad un sito web fasullo, che assomiglia a quello ufficiale, ove è chiamata ad inserire le informazioni richieste



- Dati, codici di accesso e password personali non dovrebbero mai essere comunicati.
- Se si ricevono messaggi sospetti, non cliccare sui link in essi contenuti e non aprire eventuali allegati, che potrebbero contenere virus o programmi *trojan horse* capaci di prendere il controllo di pc e smartphone.
- Posizionare sempre il puntatore del mouse sui link prima di cliccare: in molti casi si potrà così leggere in basso a sinistra nel browser il vero nome del sito cui si verrà indirizzati.



COME RICONOSCERE UN TENTATIVO DI PHISHING: LE TRE FASI DEL PHISHING ATTACK



- a) **fase 1:** invio di un messaggio di posta elettronica, contenente il link di indirizzamento alla pagina *web* non autentica, diretto ad indurre un soggetto utente o fruitore di un servizio *on line* a rivelare informazioni personali di carattere riservato;
- b) **fase 2:** "raccolta" o "pesca" dei dati riservati del soggetto utente o fruitore del servizio *on line* tramite tale sito, ovvero attraverso un *form* da compilare contenente le stringhe corrispondenti alle informazioni personali richieste;
- c) **fase 3:** utilizzo delle informazioni raccolte per accedere abusivamente ai servizi *on line* o ad aree riservate, o per utilizzare indebitamente carte di credito o di pagamento, realizzando un profitto.



COME RICONOSCERE UN TENTATIVO DI PHISHING: VERIFICARE L'IP

Utilizzando servizi web che geolocalizzano gli indirizzi IP, è possibile risalire alla città dalla quale è stata inviata l'email



iplocation.net
whatismyipadress.com
tools.keycdn.com/geo

Web

Network

- IP Location Finder
- DNS Checker
- Ping Test
- Ping IPv6 Test
- Traceroute Test
- BGP Looking Glass

Security

Other

IP Location Finder

IP LOOKUP SIMPLIFIED

IP address or hostname

122.177.110.55

Find

LOCATION	
City	Delhi
Region	National Capital Territory of Delhi (DL)
Postal code	110054
Country	India (IN)
Continent	Asia (AS)
Coordinates	28.6542 (lat) / 77.2373 (long)
Time	2022-04-11 22:19:27 (Asia/Kolkata)

NETWORK	
IP address	122.177.110.55
Hostname	abts-north-dynamic-055.110.177.122.airtelbroadband.in
Provider	Bharti Airtel Ltd., Telemidia Services
ASN	24560



CYBERSECURITY: L'ERRORE UMANO

- Password: scrivere le password sui post-it; condividerle con i colleghi...
- Distrazione (v. Phishing)
- Perdita di dispositivi forniti dall'organizzazione
- ...e in generale, quelle azioni non intenzionali - o omissioni - che causano, diffondono o permettono che una violazione di sicurezza accada.

