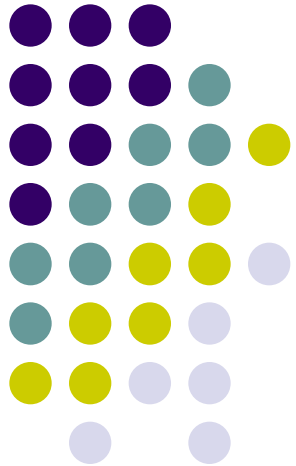
Allegato 12.
Materiale di autoformazione per Incaricati al trattamento

Maggio 2018

PBM Atletica Leggera – Bovisio Masciago

Associazione Sportiva Dilettantistica



Il nuovo regolamento UE 2016/679 Introduzione alla normativa

3 principi base

1) Trattare il minor numero di dati possibile per il minor tempo possibile
2) Distribuire le responsabilità e documentare i trattamenti
3) Favorire l'anonimizzazione e la pseudonimizzazione.

Il nuovo regolamento UE 2016/679
Introduzione alla normativa

Art. 4 n. 1 del GDPR:

“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

Il nuovo regolamento UE 2016/679
Anominimizzazione e Pseudonimizzazione

Anonimizzazione:

Forma di trattamento orientata a rendere il dato personale anonimo non riconducibile quindi all'interessato

Pseudonimizzazione:

Trattamento dei dati personali in modo tale che essi non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative per garantire che i dati non siano attribuiti a una persona identificata o identificabile (art. 4 n. 5)

Il nuovo regolamento UE 2016/679 Destinatari della normativa

Le norme interesseranno **tutti quei soggetti (anche non stabiliti nella UE, quindi extraeuropei)** che sono **chiamati a trattare** (in maniera automatizzata o meno) **i dati relativi, per esempio, a clienti, dipendenti, studenti, utenti, fornitori.**

In sostanza, viene introdotto il principio dell'applicazione del diritto dell'Unione Europea anche ai trattamenti di dati personali non svolti nell'UE, se relativi all'offerta di beni o servizi a cittadini UE o tali da comportare il monitoraggio dei loro comportamenti.

E' una **rivoluzione** rispetto alla regola precedente in base alla quale la normativa applicabile è quella del luogo in cui ha sede il Titolare del trattamento. **Ora anche soggetti non stabiliti nella UE che offrano beni/servizi alla UE sono destinatari della normativa.**

Social network, piattaforme web e motori di ricerca saranno soggette alla normativa europea anche se gestite da società con sede fuori dall'Unione Europea.

Il nuovo regolamento UE 2016/679 Introduzione alla normativa

- La legge tutela il trattamento dei dati dell'Interessato.
- La legge impone che il Titolare e il Responsabile del trattamento **adottino specifiche misure di sicurezza** per impedire l'accesso non autorizzato, il trattamento non conforme, la diffusione non autorizzata, e la dispersione e/o perdita dei dati raccolti.
- Le misure di sicurezza **si applicano ai trattamenti effettuati sia con strumenti elettronici (es.: PC) che attraverso mezzi cartacei (es.: archivi)**

Il nuovo regolamento UE 2016/679
Glossario

«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
«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

Il nuovo regolamento UE 2016/679
Cos'é il trattamento dei dati

Oggetto della tutela non è il dato in sé stesso
ma **l'utilizzo (=trattamento)** che di esso
ne farà il titolare ovvero:

- ✓ Raccolta
- ✓ Registrazione
- ✓ Organizzazione
- ✓ Conservazione
- ✓ Consultazione
- ✓ Elaborazione
- ✓ Modificazione
- ✓ Selezione
- ✓ Estrazione

- ✓ Raffronto
- ✓ Utilizzo
- ✓ Interconnessione
- ✓ Blocco
- ✓ Comunicazione
- ✓ Diffusione
- ✓ Cancellazione
- ✓ Distruzione

Esempio:

Anche la semplice visualizzazione di un dato è trattamento !

Provate ad immaginare quanti trattamenti corrispondono all'attività di redazione di un documento e alla spedizione come allegato per posta elettronica !

Il nuovo regolamento UE 2016/679
Tipi di dati

DATO PERSONALE

qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale

DATO IDENTIFICATIVO

i dati personali che permettono l'identificazione diretta dell'interessato

CATEGORIE PARTICOLARI DI DATI (GLI EX «DATI SENSIBILI»)

i 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

DATO GIUDIZIARIO

i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale

Dato personale:

- altezza, età, peso, sesso,
- indirizzo, numero di telefono

Dato identificativo:

- codice fiscale
- numero di matricola
- partita IVA

Dato sensibile:

- Paese di provenienza,
- iscrizione ad associazione politica
- stato di salute
- appartenenza a confessioni religiose

Dato giudiziario:

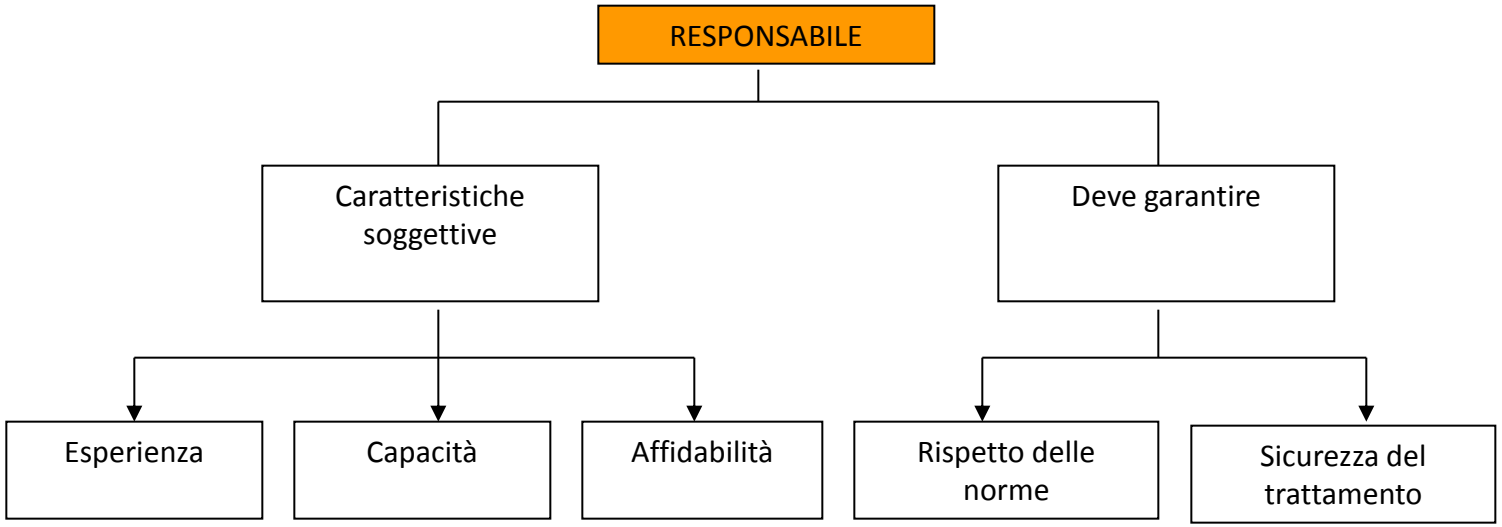
- casellario giudiziale

Il nuovo regolamento UE 2016/679
Glossario

«titolare del trattamento»:	la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.
«responsabile del trattamento»:	la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento

Il nuovo regolamento UE 2016/679
Responsabile del trattamento

- Responsabile (art. 28): è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento



Il Titolare può nominare o meno uno o più Responsabili del trattamento

Ai Responsabili del trattamento possono essere attribuiti dei compiti specifici per i trattamenti di loro competenza.

Il nuovo regolamento UE 2016/679
Glossario

«destinatario»:	**la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento**
«interessato»:	**la persona fisica cui fa riferimento il dato personale:** **- Clienti** **- Fornitori** **- dipendenti** **- collaboratori**

Il nuovo regolamento UE 2016/679
Incaricato al trattamento

- Incaricato : chiunque compie operazioni di trattamento sotto l'autorità del titolare o del responsabile. Possono essere individuati come incaricati solo le persone fisiche. La designazione degli incaricati deve ritenersi valida anche se sussiste la documentata preposizione della persona fisica ad una unità per la quale è individuato l'ambito del trattamento consentito agli addetti della medesima unità.

GLI INCARICATI

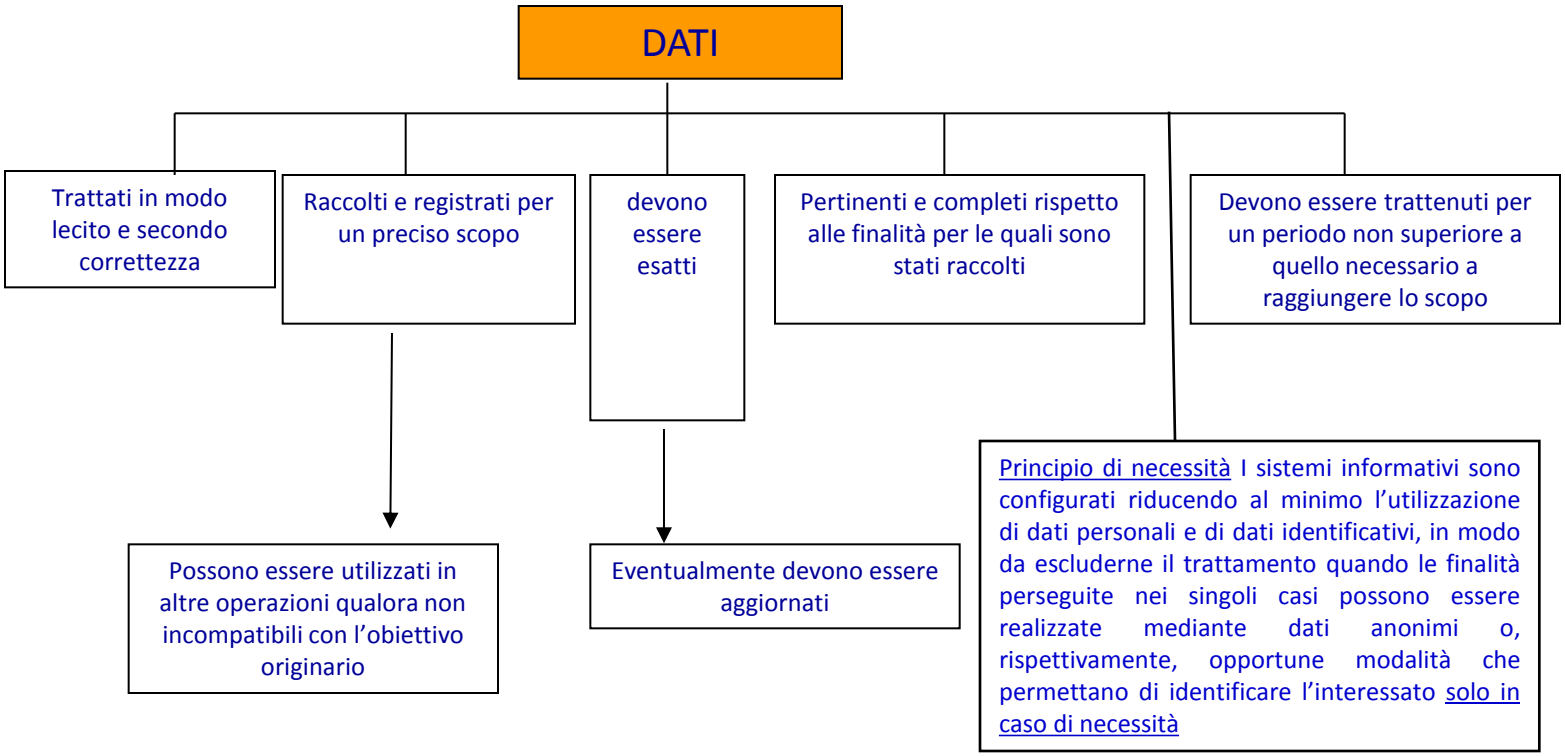
- Esistono di fatto
- Sono coloro che materialmente compiono le operazioni di trattamento
- Sono nominati dal titolare o dall'eventuale responsabile anche per mezzo di preposizione ad un'unità per la quale è individuato l'ambito del trattamento consentito
- Operano sulla base delle istruzioni (anche per mezzo di policy aziendali) impartite dal titolare o dall'eventuale responsabile
- La conoscenza da parte loro dei dati trattato non configura per la legge "comunicazione"

Tutti i dipendenti, collaboratori, consulenti, ecc. dell'azienda sono di fatto incaricati al trattamento.

Il nuovo regolamento UE 2016/679
Glossario

«violazione dei dati personali»:	**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**

Il nuovo regolamento UE 2016/679
Principi generali che regolano il trattamento



La nostra azienda tratta dati tutti i giorni! Nello stesso momento in cui un interessato fornisce dei dati all'azienda, questa comincia ad effettuare dei trattamenti che devono essere regolamentati rispetto a quanto prescrive la legge.

Il nuovo regolamento UE 2016/679
Limitazione alla conservazione

Art. 5 lett. e)

Limitazione della conservazione

Il Regolamento introduce il nuovo principio per cui "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**; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato **(«limitazione della conservazione»)**"

Il nuovo regolamento UE 2016/679 Liceità del trattamento (art. 6)

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

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

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

Il nuovo regolamento UE 2016/679
Dovere di documentazione e informazione

Sarà necessario **elaborare un sistema documentale di gestione della privacy** contenente tutti gli atti, regolarmente aggiornati, elaborati per soddisfare i requisiti di conformità al Regolamento.

Viene introdotto l'obbligo di **istituire un registro del trattamenti dei dati**

È l'applicazione operativa del **principio di rendicontazione e responsabilità** (o di "**accountability**"), secondo cui il Titolare del trattamento deve conservare la documentazione di tutti i trattamenti effettuati sotto la propria responsabilità, indicando obbligatoriamente, per ognuno di essi, una serie "nutrita" di informazioni, tali da assicurare e comprovare la conformità di ciascuna operazione alle disposizioni del Regolamento (qualcosa di simile al Documento Programmatico sulla Sicurezza, ma di portata più ampia).

Tutte le operazioni di trattamento devono essere tracciabili e documentabili.

c.d. logica della "scatola nera"

Il nuovo regolamento UE 2016/679
L'informativa

L'informativa va resa:

- in forma concisa
- trasparente
- intelligibile
- facilmente accessibile
- con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.

Il nuovo regolamento UE 2016/679
L'informativa

TITOLARE

INFORMATIVA COMPLETA
deve contenere

Interessato:
Cliente,
Fornitore,
Dipendente,
Consulente,
Collaboratore, ecc.

- Titolare, Responsabile e loro contatti
- Finalità e basi giuridiche del trattamento
- Legittimi interessi del titolare
- Destinatari o categorie di destinatari
- Periodo di conservazione
- Diritti dell'interessato (accesso, rettifica, cancellazione, limitazione, opposizione, portabilità, revoca, reclamo)
- Se la comunicazione dei dati deriva da un obbligo legale o da un obbligo contrattuale con le conseguenze della mancata comunicazione del dato
- Esistenza di processi decisionali automatizzati (profilazione)

Il nuovo regolamento UE 2016/679
Il consenso

Sono **quattro** le caratteristiche essenziali del consenso per l'uso dei dati a fini commerciali; infatti **è valida** qualsiasi manifestazione di volontà

1) Libera

2) Specifica

3) Informata

4) Inequivocabile

con la quale l'interessato accetta, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

Il nuovo regolamento UE 2016/679
Il consenso

Non è più richiesto il requisito del **consenso espresso** se non per le attività di profilazione.

Se il consenso è prestato in forma scritta per più questioni, occorre che il consenso su ogni questione sia distinguibile

Si aprono spazi maggiori per la raccolta di un **consenso manifestato** attraverso i **comportamenti positivi** dell'interessato.

Sono in ogni **caso illegittimi i consensi raccolti con caselle prebarrate**.

Il nuovo regolamento UE 2016/679
Diritti dell'interessato

Interessato:
Cliente,
Fornitore,
dipendente,
consulente,
collaboratore, ecc.

DIRITTI DELL' INTERESSATO

- Conoscere l'origine dei dati, le finalità e modalità del trattamento, la logica del trattamento informatico, l'identità del titolare, del responsabile e l'ambito di comunicazione e diffusione dei dati
- Ottenere l'aggiornamento, la modifica e/o l'integrazione dei dati, la cancellazione, la trasformazione in forma anonima e il blocco dei dati stessi
- chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati
- Proporre reclamo all'autorità di controllo
- chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati

Il nuovo regolamento UE 2016/679
Ruoli

Titolare del trattamento (art. 24) - la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali. Ha l'obblgio di porre in essere misure tecnico-organizzative adeguate

Contitolare (art. 26) – se esistono due soggetti a determinare finalità e mezzi, essi sono contitolari del trattamento

Rappresentante del titolare (art. 27) - la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare (stabilito extra UE) del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento

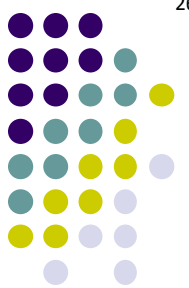
Il nuovo regolamento UE 2016/679
Ruoli

Responsabile del trattamento (art. 28) – (non è il responsabile per la protezione dei dati – art. 37 e ss.) la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un **contratto**

Sub-responsabile (art. 28) – solo se esiste autorizzazione scritta del titolare

Incaricati/Soggetti autorizzati (e tra di essi, ad es. l'Amministratore di Sistema) (art. 29) – "chiunque agisca sotto l'autorità" del responsabile o del titolare

Il nuovo regolamento UE 2016/679
Registri



Registri:

- **del titolare**
- **del responsabile**

Il nuovo regolamento UE 2016/679
Registri

Devono indicare:

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 **responsabile della protezione dei dati;**

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 od organizzazioni internazionali;

e) ove applicabile, i **trasferimenti di dati personali verso un paese terzo** o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

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 di cui all'articolo 32, paragrafo 1.

Quello del responsabile anche:

b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;

Il nuovo regolamento UE 2016/679
Registri

Sono tenuti in forma scritta, anche in formato elettronico.

Registri **non obbligatori** per le imprese o organizzazioni **con meno di 250 dipendenti**, a meno che:

a) il trattamento che esse effettuano possa presentare **un rischio per i diritti e le libertà dell'interessato,**

b) il trattamento **non sia occasionale ,**

c) il trattamento includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1 (dati personali che rivelino **l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i 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**), o i dati personali relativi a **condanne penali e a reati** di cui all'articolo 10.

Il nuovo regolamento UE 2016/679 Sicurezza del Trattamento

Chi deve garantirla?

il titolare del trattamento e il responsabile del trattamento

Come?

Mettendo in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) **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.**

Il nuovo regolamento UE 2016/679 DPO Data Protection Officer

Il Regolamento introduce la figura **del "Responsabile per la protezione dei dati" o Data Privacy Officer (DPO)**. Non è un semplice responsabile del trattamento, è il **manager del trattamento dei dati**.

Le categorie che dovranno nominarlo sono:

- Tutte le **autorità ed organismi pubblici**
- Le **imprese che trattino i dati di un rilevante numero di persone** (c.d. interessati) o tipologie di dati che per natura, oggetto o finalità siano definite categorie "a rischio" dalla normativa. persone (c.d. interessati) o tipologie di dati che per natura, oggetto o finalità siano definite categorie "a rischio" dalla normativa.

Il nuovo regolamento UE 2016/679
DPO Data Protection Officer

Chi è	Cosa fa	Quando è previsto
Figura interna o esterna all'organizzazione nominata dal titolare del trattamento e in possesso di un'adeguata conoscenza della normativa sul data protection Assenza di conflitti di interesse Ad oggi può essere certificato come da Norma ISO 17024 su schemi proprietari	Guida il titolare e il responsabile del trattamento nell'adozione degli obblighi derivanti dal GDPR Vigila sull'applicazione del GDPR Fornire se richiesto, un parere sulla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35; Interfaccia con l'autorità di controllo	Per organizzazioni pubbliche; monitoraggio regolare e sistematico degli interessati su larga scala; tutti i soggetti la cui attività principale consiste nel trattamento, su larga scala, di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici

Il nuovo regolamento UE 2016/679
Le minacce

Attacchi dall'esterno	• Acquisizione indebita di dati • Sabotaggio \ Spionaggio • Corruzione dei dati
Danni da risorse umane	• Accessi non autorizzati • Acquisizione \ Comunicazione indebita • Perdita \ Corruzione dati
Applicazioni non affidabili	• Perdita di prestazioni • Inibizione accesso ai dati • Vulnerabilità sulla sicurezza \ Fault operativi

Il nuovo regolamento UE 2016/679
Obblighi in caso di data breach

Con la nozione di violazione dei dati personali (c.d. "personal data breaches"), si intende: la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso, in modo accidentale o illecito, ai dati personali trasmessi, memorizzati o comunque elaborati.

I Titolari del trattamento, in caso di una violazione come sopra descritta, dovranno mettere in atto due differenti azioni:

1) la notificazione della violazione all'Autorità di controllo entro 72 ore dal fatto

2) la segnalazione al diretto interessato (senza ritardo ingiustificato).

Il mancato rispetto di questo obbligo comporta sanzioni penali

Il nuovo regolamento UE 2016/679
La notifica al garante

Quando: senza ingiustificato ritardo e, ove possibile, entro 72 ore dalla conoscenza.

A chi: all'autorità di controllo (Garante competente per territorio)

Contenuti della notifica:

a) descrivere la **natura della violazione** dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) comunicare il nome e i dati di contatto del **responsabile della protezione** dei dati o di altro punto di contatto presso cui ottenere più informazioni;

c) descrivere le **probabili conseguenze** della violazione dei dati personali;

d) descrivere le **misure adottate** o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Il nuovo regolamento UE 2016/679
La notifica all'interessato

Quando? Quando la violazione dei dati personali è suscettibile di presentare un **rischio elevato per i diritti e le libertà delle persone fisiche,** il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

Come? Descrivendo con un **linguaggio semplice e chiaro** la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).

Contenuti della notifica:

b) comunicare il nome e i dati di contatto del **responsabile della protezione** dei dati o di altro punto di contatto presso cui ottenere più informazioni;

c) descrivere le **probabili conseguenze** della violazione dei dati personali;

d) descrivere le **misure adottate** o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Nessuna comunicazione se, alternativamente:

a) il titolare del trattamento ha **messo in atto le misure tecniche e organizzative adeguate** di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) il titolare del trattamento ha **successivamente adottato misure atte a scongiurare** il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;

c) detta comunicazione richiederebbe **sforzi sproporzionati**. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Il nuovo regolamento UE 2016/679
Nuovi diritti

Il testo del Regolamento riconosce nuovi diritti agli interessati. In particolare si fa riferimento a:

1) **Diritto all'oblio (right to be forgotten / right to erasure)**
2) **Diritto alla portabilità del dato (data portability)**

Il nuovo regolamento UE 2016/679 Diritto all'Oblio

L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste **uno dei motivi** seguenti:

a) i dati personali **non sono più necessari rispetto alle finalità** per le quali sono stati raccolti o altrimenti trattati;

b) l'interessato **revoca il consenso** su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;

c) l'interessato **si oppone al trattamento** ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;

d) i dati personali **sono stati trattati illecitamente**;

e) i dati personali devono essere cancellati **per adempiere un obbligo legale** previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;

f) i dati personali sono stati **raccolti relativamente all'offerta di servizi della società dell'informazione** di cui all'articolo 8, paragrafo 1.

Il nuovo regolamento UE 2016/679
Diritto alla portabilità dei dati

Con Diritto alla portabilità del dato si intende il riconoscimento sia del diritto dell'interessato a trasferire i propri dati (es. quelli relativi al proprio "profilo utente") da un sistema di trattamento elettronico (es. Social Network) ad un altro senza che il Titolare possa impedirlo, sia del diritto di ottenere gli stessi in un formato elettronico strutturato e di uso comune che consenta di farne ulteriore uso.

Tale diritto deve sempre trovare applicazione quando:

a) Il trattamento si basa sul consenso

b) Il trattamento sia effettuato con mezzi automatizzati

Il nuovo regolamento UE 2016/679
Le Sanzioni

Diventano molto più severe:

- Fino a € 20.000.000 per i privati e le imprese non facenti parte di gruppi.

- Fino al 4% del fatturato complessivo (consolidato) per i Gruppi societari

Si tratta di un cambio di passo significativo.

Le sanzioni sono pensate per incidere sulle condotte dei grandi gruppi multinazionali che trattano dati in diverse aree geografiche e spesso cercano di individuare i paradisi legali del trattamento dei dati personali per eludere norme e criteri di comportamento definiti dalle nazioni più rigorose.

Il nuovo regolamento UE 2016/679 Titolare, Responsabile, Incaricato

Dato personale
Dato identificativo
Dato sensibile
Dato giudiziario

Interessato:
Cliente,
Fornitore,
Dipendente,
Consulente,
Collaboratore, ecc.

TITOLARE

Dati dell'interessato

Trattamenti effettuati:

- ✓ Raccolta
- ✓ Registrazione
- ✓ Organizzazione
- ✓ Conservazione
- ✓ Consultazione
- ✓ Elaborazione
- ✓ Modificazione
- ✓ Selezione
- ✓ Estrazione
- ✓ Raffronto
- ✓ Utilizzo
- ✓ Interconnessione
- ✓ Blocco
- ✓ Comunicazione
- ✓ Diffusione
- ✓ Cancellazione
- ✓ Distruzione

Responsabili ed Incaricati

Ai trattamenti vanno applicate le misure di sicurezza !

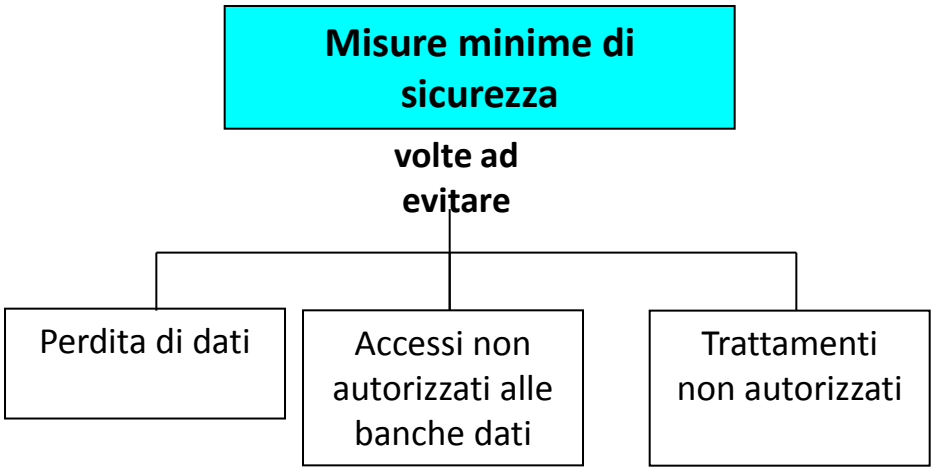
Le misure di sicurezza

<u>Le misure di sicurezza sono suddivise in:</u>

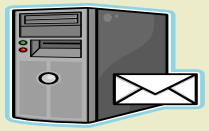
- **Idonee** , cioè quelle che il titolare e/o il responsabile applicano anche sfruttando al meglio le tecnologie esistenti
- **Minime**, cioè quelle richieste per legge e da applicarsi obbligatoriamente

<u>Attenzione:</u> **la legge prevede che il titolare debba aggiornare le misure al meglio della tecnologia disponibile tenendo conto della natura dei dati e dei trattamenti effettuati alla luce dei rischi**

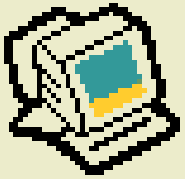
Adozione di idonee e preventive misure di sicurezza anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.



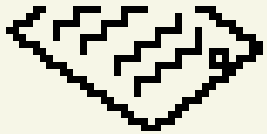
Le misure di sicurezza (1 di 3)

Misura di sicurezza	Obiettivo	Cosa devo fare ?
Autenticazione 	Verificare l'identità di colui che utilizza il PC	Devo fornire le mie credenziali di accesso per accedere a tutti i PC.
Antivirus 	Eliminare i virus presenti in messaggi e documenti	Nulla. Il sistema è automatico e viene gestito dal Servizio IT.
Antispam 	Eliminare la posta indesiderata	Nulla se ho richiesto l'attivazione. Il sistema viene gestito dal Servizio IT

Le misure di sicurezza (2 di 3)

Misura	Obiettivo	Cosa devo fare?
Screen Saver: 	Evitare che i dati siano visualizzati da estranei durante l'assenza dell'incaricato	Devo fornire le mie credenziali di accesso, perché dopo un determinato periodo di non utilizzo il PC si blocca.
Aggiornamenti: 	Applicare modifiche al software di sistema ed applicativo per ridurre il rischio di errori e/o intrusioni	Nulla. Il sistema è automatico e viene gestito dal Servizio IT.
Firewall 	Evitare che dall'esterno (Internet) si acceda in modo fraudolento o non autorizzato ai sistemi della G.Bozzetto	Nulla. Il sistema è automatico e viene gestito dal Servizio IT.

Le misure di sicurezza (3 di 3)

Misura	Obiettivo	Cosa devo fare
Blocco del PC 	Evitare che la configurazione del PC (hardware e/o software) venga inavvertitamente modificata riducendo il livello di sicurezza dei sistemi	Nulla. Il sistema è automatico e viene gestito dal Servizio IT.
Linee Guida per un corretto utilizzo degli strumenti elettronici 	Dare istruzione agli incaricati affinché sappiano come comportarsi e riducano i rischi di sicurezza	**Adottare le Linee Guida ed in caso di dubbi contattare il proprio Responsabile di funzione**

Procedura di autenticazione (1 di 2)

Credenziali		Esempio:
Userid	+	RossiM
Password		P@ssw0rd

Le credenziali sono assegnate dal Servizio IT. Devono essere utilizzate su tutti i PC dell'azienda. Se un PC risulta accessibile senza aver bisogno di digitare le credenziali avvisare subito il servizio IT.

Procedura di autenticazione (2 di 2)

Credenziali

- Userid
- Password

Dopo tre (3) tentativi di accesso con password e/o userid errato il sistema si blocca !

Chiamare il servizio IT per farsi riabilitare le credenziali

Caratteristiche delle credenziali (1 di 3)

Password

Lunghezza minima 8 caratteri

Almeno 1 numero o car. speciale (#@!”£$%&/()=?^*§1234567890)

Almeno 1 carattere maiuscolo (ABCDEFGHILMNOPQRSTUVZ)

Almeno 1 carattere minuscolo (abcdefghilmnopqrstuvz)

NESSUNO deve conoscere la vostra password oltre a Voi.

Nemmeno il Servizio IT conosce la vostra password.

Caratteristiche delle credenziali (2 di 3)

Password

- E’ strettamente personale !
- Non è cedibile ! E’ la vostra garanzia di sicurezza !
- Scadenza automatica dopo 40 giorni.
- Non sono utilizzabili le ultime 3 password inserite !

Caratteristiche delle credenziali (3 di 3)

Password consigliate	Password NON consigliate
P@ssword **1234Ciao** **Nonlad1co** **!Domani!** **#Gennaio#**	**miapass** (non contiene numeri o caratteri speciali, non contiene caratteri maiuscoli ed è di lunghezza inferiore a 8 caratteri) **miapass1** (contiene numeri ma non caratteri maiuscoli) **01234567** (non contiene lettere maiuscole e minuscole)

Antivirus

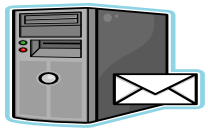
Non disattivare mai il Vs. antivirus !

Sistema automatico

Aggiornato dall'IT

Il software antivirus controlla automaticamente la presenza di virus nei documenti e nei file

AntiSpam



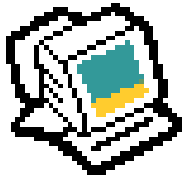
Se attivato, Il sistema controlla automaticamente la posta elettronica ricevuta dall'azienda.

Sistema automatico

Aggiornato dall' IT

Il software antispam controlla automaticamente la presenza di posta indesiderata. È sempre consigliabile controllare le mail filtrate. I software antispam non sono infallibili.

Screen Saver

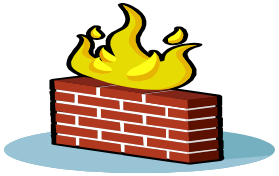


Sistema automatico

Si attiva automaticamente dopo un predeterminato periodo di inattività

Per riaccedere al PC ridigitare Userid e Password

Firewall



Sistema automatico

Dispositivo installato centralmente sulla rete dell'azienda

Controlla automaticamente tutto il traffico da / verso Internet

Aggiornamenti

Sistema automatico

Sui Pc: viene automaticamente installato l'aggiornamento più adatto.

Sui Server: Il servizio IT provvede agli aggiornamenti in funzione delle necessità

Linee Guida

Da leggere e comprendere

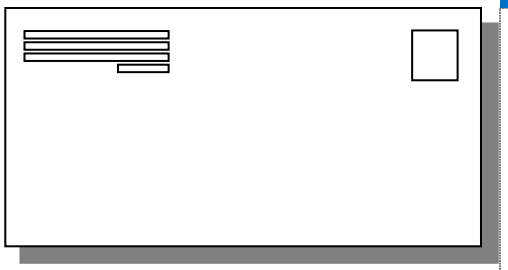
Vengono aggiornate costantemente.

Possono fare riferimento a procedure di comportamento specifiche.

Verranno pubblicate nell'area comune (cartella/intranet): ……

Per qualsiasi dubbio parlate con il Vostro Responsabile di funzione.

Email:regole generali



Evitare di:

- Spedire email con documenti aziendali a mittenti non conosciuti o incerti
- Utilizzare la posta elettronica per comunicazioni personali.
- Rispondere alle catene di Sant'Antonio.
- Esprimere giudizi in nome e per conto dell'azienda, senza la necessaria autorizzazione del Responsabile di funzione.

Internet: regole generali

Evitare di:

- Scaricare da Internet giochi, programmi, filmati, file, ecc.
- Utilizzare Blog, chat, forum di discussione, ecc.
- Navigare su siti non pertinenti con le mansioni affidate
- Pubblicare e/o fornire su Internet dati dell'azienda, in qualsiasi forma essa siano.
- Non utilizzare il PC aziendale per attività ludiche, a scopo di lucro e comunque legate a trasferimento di beni e/o servizi tramite Internet (es**.: EBAY VIETATO!!)**
- Utilizzare siti di social network quali www.live.it www.facebook.com, www.twitter.com, ecc.

File: regole generali

Evitare di:

- Archiviare materiale che abbia riferimenti o attinenze con l'aspetto politico e/o religioso
- Archiviare materiale che non sia riconducibile ad attività di tipo personale
- Archiviare materiale ludico e/o di intrattenimento(giochi, utilities, sfondi, fotografie, immagini, ecc.)
- Salvare materiale soggetto alla legislazione nazionale ed internazionale sul diritto d'autore(file mp3, file video), sulla proprietà intellettuale, sui brevetti, ecc.