AiFOS Convention 2018

14 e 15 giugno 2018

West Garda Hotel

Padenghe sul Garda BS

Relatore: Sebastiano Plutino

A Partner of VISION ZERO Safety.Health.Wellbeing

CONFCOMMERCIO

CIIP

Media Partner

PuntoSicuro

AMBIENTE&SICUREZZA

I professionisti della privacy

AiFOS

GDPR: il percorso verso la conformità

L’alba in un mare agitato

AiFOS

25 maggio 2018

AiFOS

Sebastiano Plutino

Socio AiFOS, Auditor SGQ AiFOS

Esperienze in ambito Protezione Dati Personali:

- *…. mi chiamano solo se ci sono situazioni complesse….*
- *… mi piace trovare la soluzione più adatta per il cliente*

AiFOS

Il Regolamento EU 679/2016

Questo conosciuto…

AiFOS

Fonti di diritto derivato: due strumenti della UE

Le DIRETTIVE

Sono indirizzate solo agli Stati membri e non sono obbligatorie in tutti i loro elementi, in quanto vincolano i destinatari solo riguardo al risultato da raggiungere, lasciando alla loro discrezione la scelta dei mezzi e della forma

I REGOLAMENTI

Hanno una portata generale, sono obbligatori in tutti i loro elementi e direttamente applicabili

Il Regolamento - La normativa

AiFOS

Le istituzioni UE hanno colto l'importanza della Protezione dei Dati Personali e hanno affrontato la tematica tramite:

- **Direttiva 95/46 CE (Tutela e libera circolazione dei dati personali)**
- Direttiva 2000/31/CE («Direttiva sul commercio elettronico»)
- Direttiva 2002/58 CE (Telecomunicazioni)
- Direttiva 2006/24 CE (Conservazione di dati)
- Decisione quadro 977/2008 (dati scambiati dalle autorità di polizia)
- Direttiva 2009/136 CE (E-Privacy)
- …

I testi dei documenti sono disponibili nel sito http://eur-lex.europa.eu

Il Regolamento - La normativa

AiFOS

In Italia la direttiva 95/46 CE è stata recepita tramite il

D.Lgs. 196 del 30 giugno 2003

Codice in materia di protezione dei dati personali

Il testo del Codice Privacy è disponibile nel sito http://www.garanteprivacy.it

Il Regolamento: Chi controlla

AiFOS

Il *Codice della Privacy*

ha, tra le altre, disciplinato

l'***Autorità Garante per la protezione dei dati personali***

(G.P.D.P.)

autorità amministrativa indipendente che si occupa di tutti gli ambiti, pubblici e privati, nei quali occorre assicurare il corretto trattamento dei dati e il rispetto dei diritti delle persone connessi all'utilizzo delle informazioni personali.

Il Regolamento: Chi controlla

AiFOS

1997 2017

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

A TUTELA DI UN DIRITTO FONDAMENTALE

Il Presidente dell'Autorità Garante Antonello Soro

attraverso

Guardia di Finanza - Nucleo Speciale Privacy

Sede: ROMA
Prov.: RM
C.a.p.: 00155
Indirizzo: Via Fortunato Depero, 76
Telefono: 06225941

La cultura della protezione dei dati personali

AiFOS

La cultura della protezione dei dati personali è prioritaria perché connessa alle libertà fondamentali della **Carta Costitutiva dell'Unione**.

Trattato di Lisbona

- **Un'Europa di diritti e valori, di libertà, solidarietà e sicurezza,** che promuove i valori dell'Unione, integra la Carta dei diritti fondamentali nel diritto primario europeo, prevede nuovi meccanismi di solidarietà e garantisce una migliore protezione dei cittadini europei.
- Il trattato di Lisbona mantiene i diritti esistenti e ne introduce di nuovi. In particolare, garantisce le libertà e i principi sanciti dalla Carta dei diritti fondamentali rendendoli giuridicamente vincolanti. Il trattato contempla diritti civili, politici, economici e sociali.
- Libertà dei cittadini europei: il trattato di Lisbona mantiene e rafforza le quattro libertà fondamentali, nonché la libertà politica, economica e sociale dei cittadini europei.

«L'Unione si fonda sui valori indivisibili e universali della dignità umana, della libertà, dell'uguaglianza e della solidarietà; essa si basa sul principio della democrazia e sul principio dello stato di diritto»

(Nizza 7/12/2000 – Strasburgo 12/12/2007 – Lisbona 13/12/2007)

Antefatti

AiFOS

Nel **1995** la Comunità Europea emette la Direttiva 46/CE avente per oggetto la «***Tutela e libera circolazione dei dati personali***»

- Gli stati membri recepiscono la direttiva con leggi nazionali
- In Italia Legge n. 675/1996 - Dlgs. 196/2003 (Codice Privacy) e smi

Nel **gennaio 2012** la Commissione Europea ha presentato ufficialmente il «**pacchetto protezione dati**», con l'intento di «rafforzare i diritti delle persone fisiche con riguardo alla protezione dei dati e agevolare la libera circolazione dei dati personali nel mercato unico digitale»

Il Regolamento - La normativa

AiFOS

Rispetto alla normativa di base adottata oltre 20 anni fa sono intervenuti:

1. Cambiamenti nel contesto

- Fenomeno della globalizzazione
- Nuove tecnologie
- Nuovi servizi collegati alle nuove tecnologie

2. Frammentazione e disomogeneità del quadro normativo

- Tempi e modi diversi, da parte dei 28 paesi membri, di recepire la direttiva 95/46 CE e le successive norme
- Provvedimenti in materia Privacy adottati dai singoli stati
    - Stessi diritti, stessi doveri
    - Concorrenza leale
    - Confronto paritetico

Per dare una risposta ai due punti nasce la nuova normativa europea …

Il 27 aprile 2016, il Parlamento Europeo …

AiFOS

approva il «pacchetto protezione dati», contenente:

- il **Regolamento**, (UE) 2016/679 del Parlamento europeo e del Consiglio, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);

- la **Direttiva**, (UE) 2016/680 del Parlamento europeo e del Consiglio, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

AiFOS

25 MAGGIO 2018

totalmente applicabile il

REGOLAMENTO (UE) 679/2016

DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 27 aprile 2016

relativo alla **protezione delle persone fisiche** con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

Panoramica - Regolamento Europeo 679/2016

AiFOS

25 maggio 2018

A partire dal 25 maggio 2018, il Regolamento Europeo 679/2016 sulla protezione dei dati personali è applicabile in tutti i paesi appartenenti allo spazio economico europeo.

Il dato personale è la persona e come tale va rispettato. La persona affida se stessa e l'affidatario deve attribuire il massimo rispetto.

La protezione dei dati personali è uno dei più importanti doveri di ogni organizzazione o ente – pubblico o privato – che tratta, a qualunque titolo, informazioni personali.

AiFOS

… e il Codice della Privacy che fine fa?

… ma ci sarà una proroga?

Il Regolamento - La normativa

AiFOS

GDPR, Garante privacy: nessuna pronuncia su differimento applicazione sanzioni

Con riferimento a notizie circolanti in Internet è necessario precisare che non è vero che il Garante per la protezione dei dati si sia pronunciato sul differimento dello svolgimento delle funzioni ispettive e sanzionatorie né il provvedimento richiamato nei siti attiene a tale materia.

Nessun provvedimento del Garante, peraltro, potrebbe incidere sulla data di entrata in vigore del Regolamento europeo fissata al 25 maggio 2018.

Roma, 19 aprile 2018

Presentazione dell'Autorità Garante ai DPO – Bologna 24 maggio 2018:

«Il Regolamento sarà pienamente operativo dal 25 maggio 2018 – L'Autorità Garante effettua i controlli secondo un programma definito. Al momento il programma non è ancora stato definito. Tuttavia l'Autorità reagirà in caso di richieste degli Interessati.»

AiFOS

Il Regolamento

- definisce i principi
- governa i rapporti tra i vari attori coinvolti

Ha come fine la tutela delle libertà fondamentali delle persone fisiche partendo dai loro dati personali

Il Regolamento Aspetti generali

AiFOS

Articolo 1

1. Il regolamento stabilisce norme relative alla **protezione delle persone fisiche** con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati.
2. Il regolamento **protegge i diritti e le libertà fondamentali delle persone fisiche**, in particolare il diritto alla protezione dei dati personali.

Articolo 2 (ambito materiale)

Il regolamento si applica al **trattamento** interamente o parzialmente automatizzato **di dati personali** e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.

I dati riferiti a società non sono dati personali

AiFOS

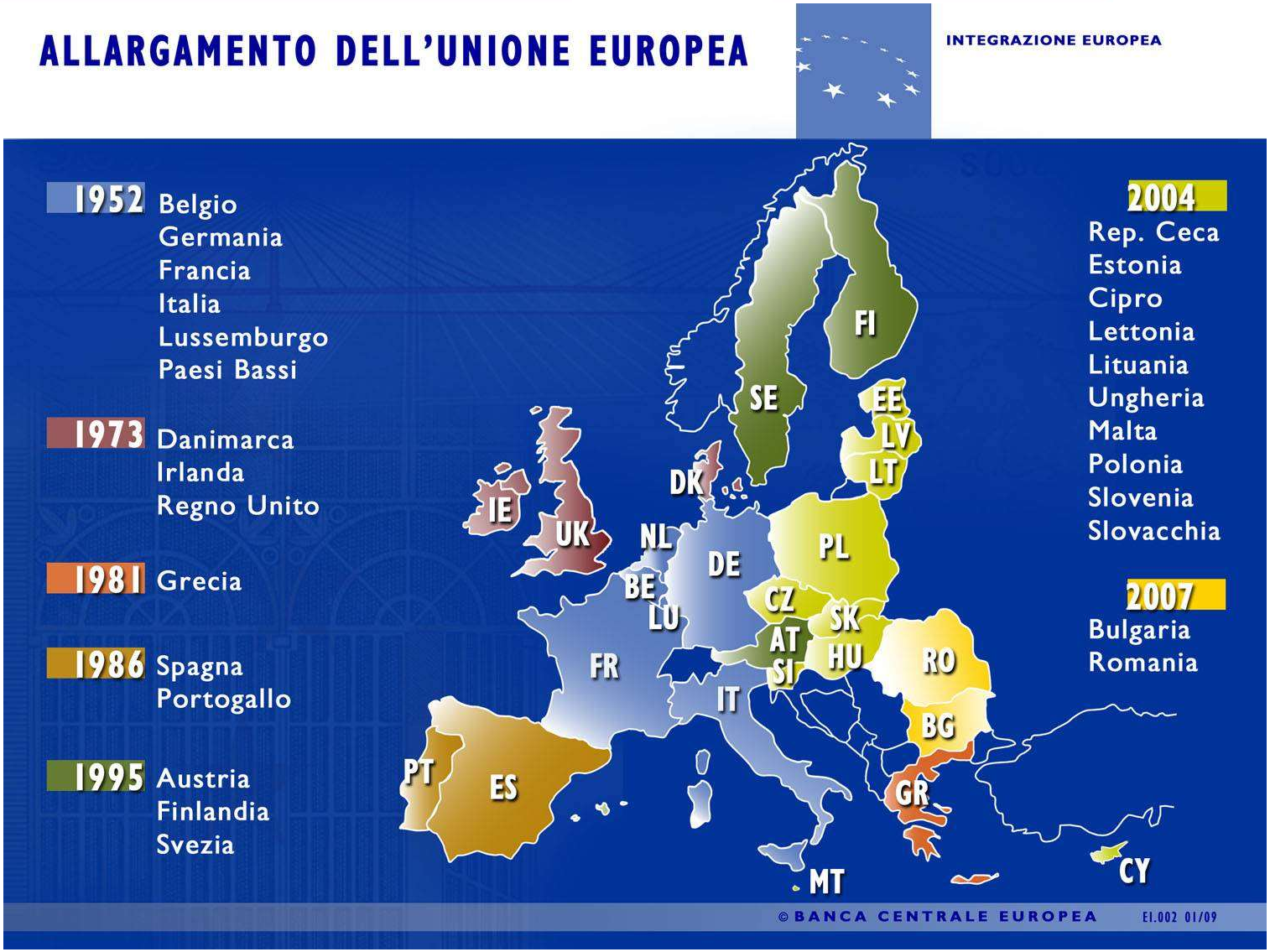
Articolo 3

Ambito Territoriale

1. Il regolamento si applica al **trattamento dei dati personali** effettuato nell'ambito delle attività di uno **stabilimento** da parte di un titolare del trattamento o di un responsabile del trattamento sito nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione;
2. Il regolamento si applica al **trattamento dei dati personali di interessati che si trovano nell'Unione**, effettuato da un titolare del trattamento o da un responsabile del trattamento che **non è stabilito nell'Unione**, per offerta di beni o la prestazione di servizi oppure che attui il monitoraggio del loro comportamento all'interno dell'Unione;
3. Il regolamento si applica al trattamento dei dati personali effettuato da un **titolare del trattamento che non è stabilito nell'Unione** in un luogo **soggetto al diritto di uno Stato membro dell'Unione**.

Il Regolamento - Aspetti generali

AiFOS

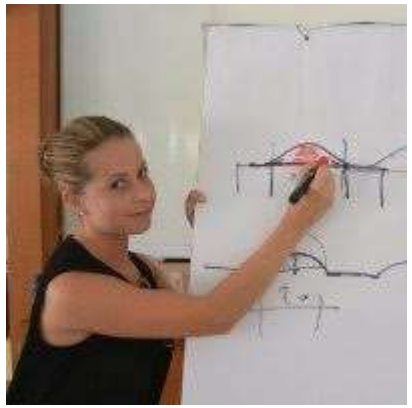


AiFOS

Articolo 4

Il 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.



Le norme: La definizione di dati personali

AiFOS

Secondo la normativa internazionale sono definibili DATI PERSONALI:

Nome
Data di nascita

Identificativi nazionali (ad es. Numero di passaporto)
Indirizzo e-mail personale
Numero di telefono personale
Numeri di identificazione personale (PIN) o password

Genere
Età o bisogni speciali delle persone fisiche vulnerabili

Identificatore biometrico
Informazioni sanitarie diagnostiche
disabilità
Fatture del medico
Qualsiasi informazione raccolta durante i servizi sanitari
Storia medica

Fotografia o video identificabili con una persona fisica

Origine razziale o etnica
Credenze religiose o filosofiche
Orientamento sessuale
Appartenenza sindacale

Posizione GPS
Traiettorie GPS
Indirizzo di casa
indirizzo IP
Posizione derivata dai sistemi di telecomunicazione
Interessi personali derivati dall'utilizzo di tracciamento di siti Web

Profilo personale o comportamentale

Conto bancario o numero di carta di credito
Estratto conto della carta di credito
Profilo finanziario

Numero cliente
Bollette
Preferenze di prodotto e servizio

Accuse di condotta criminale
Condanne penali o infrazioni commesse
Rapporti di indagini penali

Rif. ISO/IEC 29100

Il Regolamento UE 2016/679 …

AiFOS

- ✓ È **in vigore dal 25 maggio 2016** (20 giorni dopo la pubblicazione, sulla Gazzetta dell'unione europea, avvenuta il *4 maggio 2016*)
- ✓ Non ha necessità di normative nazionali per il recepimento e diventa obbligatoria l'**applicazione** a partire dal **25 maggio 2018**.

Che ha detto l'Autorità?

- ✓ È **valido in tutta Europa**
- ✓ Riguarda **tutte le organizzazioni che offrono servizi ai cittadini Europei,** (quindi anche quelle stabilite fuori dal territorio Europeo)
- ✓ La Direttiva 95/46/CE, a decorrere dalla stessa data, è abrogata; ***tutti i riferimenti nazionali devono intendersi «trasferiti» al Regolamento, incluso il Codice Privacy italiano*** *(Dlgs 196/2003)*
- ✓ **È stato concesso alle imprese il tempo necessario per compiere il percorso di adeguamento** e arrivare al **25 maggio 2018** in una situazione di pieno rispetto normativo

Elementi chiave del Regolamento (a)

AiFOS

- **DIMOSTRARE**, in caso di controlli o reclami, di aver preso **DECISIONI PONDERATE** e di aver agito per tutelare i diritti e le libertà dell'interessato

- **ADOTTARE misure tecniche e organizzative ADEGUATE** allo specifico contesto

- **DOCUMENTARE** le decisioni prese e **CONSERVARNE l'EVIDENZA.** Sarà fondamentale per dimostrare la diligenza del «buon padre di famiglia»

- **COMUNICARE** con gli **INTERESSATI** in modo **chiaro, specifico e comprensibile**

- **VALUTARE attentamente i propri RISCHI e le proprie opportunità** (approccio «sistema di gestione» per le Organizzazioni che ne sono dotate)

Elementi chiave del Regolamento (b)

AiFOS

Il Regolamento **non fornisce**:

- soluzioni «standard», buone per tutte le situazioni
- check-list
- ricette replicabili in ogni contesto

né impone misure particolari.

Soluzioni Adeguate
Scelte responsabilmente

Accountability

Ogni Titolare che ha cura della propria organizzazione deve scegliere la soluzione adeguata

AiFOS

Il quadro sanzionatorio (art. 83)

Il nuovo Sistema Sanzionatorio:

- Il sistema sanzionatorio è di tipo amministrativo.
- Le sanzioni devono essere **effettive, proporzionate e dissuasive** (considerando 152);
- *il sistema sanzionatorio penale è demandato all'autonomia degli Stati*;

Sanzioni amministrative pecuniarie **fino a 10.000.000 € o**, per le imprese, **fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente** per violazioni relative a:

- ❑ obblighi del Titolare e del Responsabile
- ❑ obblighi dell'organismo di certificazione
- ❑ obblighi dell'organismo di controllo

fino a 10.000.000 € - 2% del fatturato mondiale

Sanzioni amministrative pecuniarie **fino a 20.000.000 € o**, per le imprese, **fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente** per violazioni relative ai:

- ❑ principi di base del trattamento, comprese le condizioni relative al consenso
- ❑ diritti degli interessati
- ❑ trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale

fino a 20.000.000 € - 4% del fatturato mondiale

Elementi chiave del Regolamento (d)

AiFOS

Le aree di principale novità

- Comunicazioni trasparenti
- Notifica di violazioni
- Dimostrazione della conformità & *accountability*
- Sicurezza del trattamento estesa a tutti gli attori coinvolti
- Gestione del rischio e valutazione d'impatto
- Utilizzo di cloud (trasferimento dati)
- Risorse adeguate e informate
- «Nuovi» Documenti (Registro dei Trattamenti)
- Nomina del Data Protection Officer
- Sanzioni rilevanti e dissuasive

AiFOS

Il Regolamento EU 679/2016

Questo sconosciuto…

Panoramica - Regolamento Europeo 679/2016

AiFOS

Contesto in evoluzione

Nuovi servizi abilitati da nuove tecnologie

- Le evoluzioni tecnologiche, impensabili solo qualche hanno fa, abilitano la disponibilità di nuovi servizi grazie alla possibilità di scambiare e elaborare grandi quantità di dati personali
- La grande quantità di dati personali circolanti e i servizi innovativi correlati (IOT, APPS,…) non devono mettere a rischio i diritti dell'individuo

Valore delle informazioni personali per il mercato

- I dati personali sono un patrimonio fondamentale sul mercato e una fonte di valore e di profitto per le organizzazioni in termini di:
  - capacita di predizione e supporto alle decisioni strategiche
  - miglioramento della soddisfazione dei clienti
  - marketing e collocamento dei prodotti sul mercato

Panoramica - Regolamento Europeo 679/2016

AiFOS

Gli attori principali

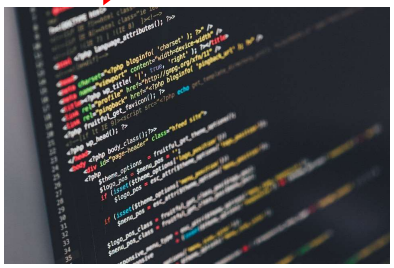
Interessati

Titolare del Trattamento

Decide finalità e mezzi del trattamento

Autorità

Controlla il rispetto delle libertà fondamentali



Responsabile del Trattamento

Tratta dati personali per conto del Titolare del trattamento su specifica nomina e con istruzioni precise

Panoramica - Regolamento Europeo 679/2016

AiFOS

Una figura innovativa – Il Responsabile della Protezione Dati – DPO - RPD

È una **figura di garanzia**, già contemplata da alcune legislazioni europee, introdotta in Italia dal Regolamento.

È designato in funzione delle **qualità professionali**, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei Dati Personali e della capacità di assolvere i compiti previsti dal Regolamento.

Panoramica - Regolamento Europeo 679/2016

AiFOS

INTERESSATI - Diritti dell'individuo

Difesa dei diritti e delle libertà fondamentali degli individui

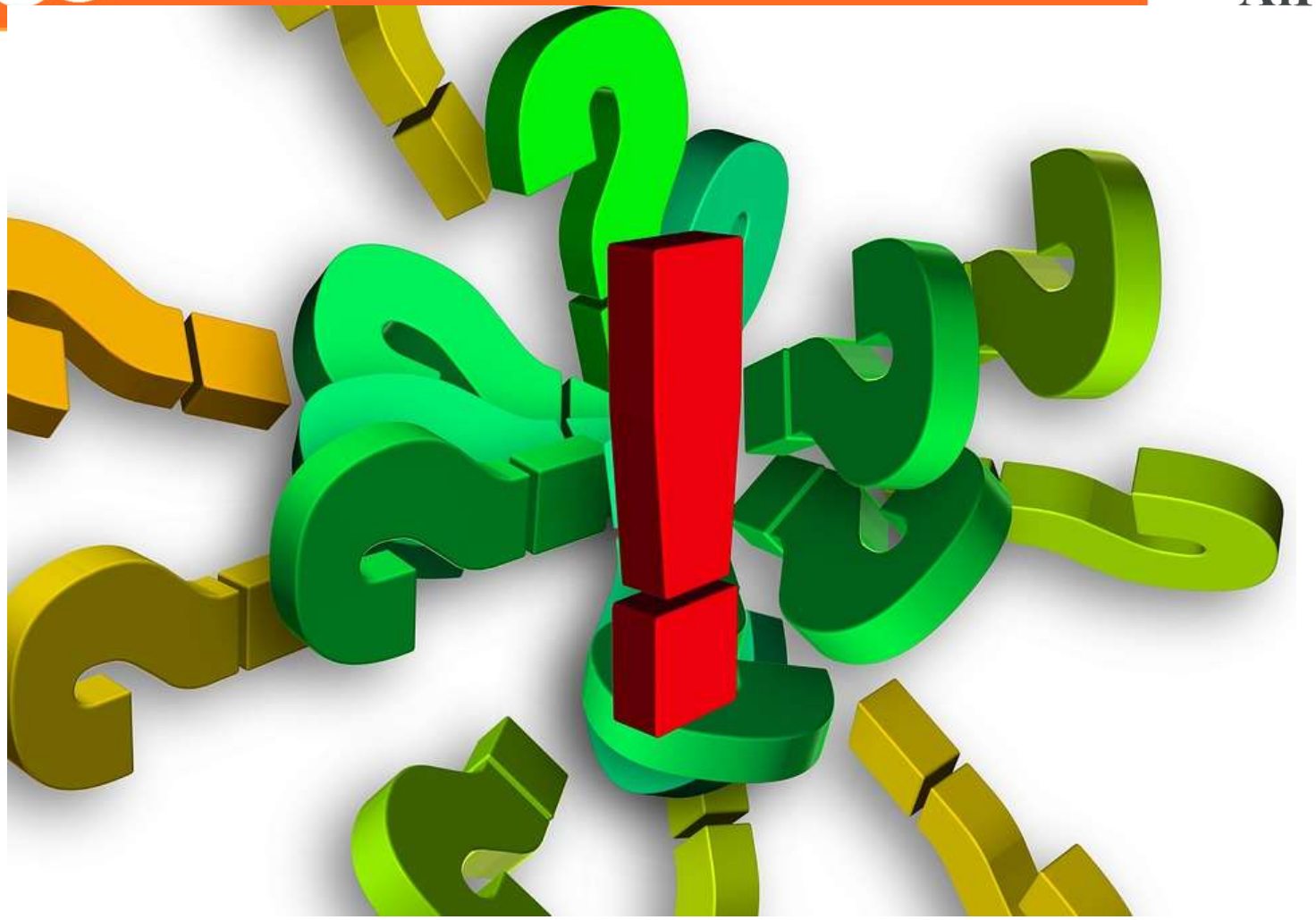
- Ciascuno deve essere **informato chiaramente** in merito alle finalità e alle modalità del trattamento dei propri dati e alle garanzie di protezione con quali garanzie di protezione
- Scongiurare l'utilizzo **illegale** o **improprio** di dati personali e le possibili **discriminazioni**

Risposta tempestiva in caso di esercizio dei diritti

- Accesso
- Rettifica
- Cancellazione (oblio)
- Limitazione al trattamento
- Portabilità dei dati
- Opposizione
- Intervento umano in processi decisionali automatizzati

Domande o commenti

AiFOS



Slurp!!!!

AiFOS

Buon pranzo….

Pizza.....

AiFOS

Pare che l'abbiocco scatti verso le 15:27 ….
Abbiamo un po' di tempo

Panoramica - Regolamento Europeo 679/2016

AiFOS

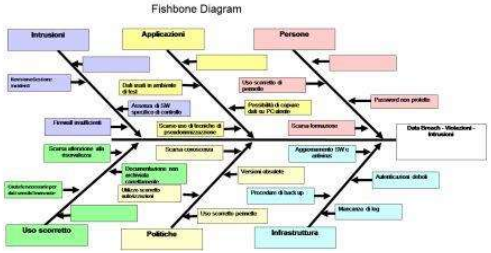
IL TITOLARE – IL RESPONSABILE - *LE IMPRESE* (1)

A chi si applica

- **Imprese con sede in UE** che trattano dati personali di individui collocati nel territorio europeo indipendentemente dal luogo di trattamento
- **Imprese con sede extra-UE**, quando le attività di trattamento riguardano:
  a) l'offerta di beni o la prestazione di servizi, anche gratuita, a individui collocati in UE;
  b) il monitoraggio del comportamento di individui nella misura in cui tale comportamento ha luogo all'interno dell'Unione.

Accountability

- Le imprese sono **responsabili** e **rendono conto di quello** che fanno (decisioni, azioni, affidamento di incarichi) in merito agli obblighi a lui assegnati dalla normativa
- Tengono conto dei **rischi associati** al trattamento e dimostrano, con **evidenze**, le ragioni delle loro scelte e delle azioni intraprese per garantire la sicurezza
- Ruolo centrale assegnato alla corretta gestione del rischio



AiFOS

IL TITOLARE – IL RESPONSABILE - *LE IMPRESE* (2)

Mantenimento della reputazione

- Enti e imprese (organizzazioni) possono subire importanti **conseguenze sulla loro reputazione** in caso di violazioni alla norma o, ad esempio, nel caso di violazioni di dati personali
- Conseguenze possibili sono **perdita di credibilità** sul mercato e riduzione del giro d'affari

Evitare costi per la non conformità

- Enti e imprese non conformi possono subire **sanzioni fino a un massimo di 20 milioni di € o fino al 4% del fatturato annuale** a livello mondiale
- Il valore della sanzione tiene conto dei **comportamenti** e delle **misure adottate** dall'organizzazione in merito alla protezione dei dati personali

Panoramica - Regolamento Europeo 679/2016

AiFOS

Alcuni informazioni …..

Violazioni in aumento

- Le minacce diventano ogni giorno più sofisticate e sono in grado di causare danni finanziari su scala mondiale
- La quasi totalità degli attacchi ha obiettivi finanziari precisi; nel caso di enti o agenzie pubbliche il danno principale è la reputazione
- Gli analisti prevedono che gli attacchi continueranno a crescere

Cause delle violazioni

- Se si escludono gli eventi legati a azioni mirate di hacker, molti incidenti accadono:
  - per negligenze o disattenzioni
  - per mancata adozione di cautele elementari o mancato rispetto dei comportamenti raccomandati
  - per errata valutazione delle priorità aziendali o ritardi nell'attuazione di misure elementari di protezione

Principi e definizioni

AiFOS

PRINCIPIO: I dati personali devono essere

- trattati in modo **lecito, corretto e trasparente** nei confronti dell'interessato
- raccolti per **finalità determinate**, esplicite e legittime
- esatti e, se necessario, aggiornati; ovvero cancellati o rettificati tempestivamente rispetto alle finalità per le quali sono trattati
- **adeguati, pertinenti e limitati** a quanto necessario rispetto alle finalità per le quali sono trattati
- **conservati** in modo da consentire l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati
- trattati in maniera da garantirne un'adeguata **sicurezza**

liceità, correttezza e trasparenza	**minimizzazione dei dati**
limitazione della finalità	**limitazione della conservazione**
esattezza	**riservatezza**

Il titolare del trattamento è competente per il rispetto di questi principi fondamentali ed è in grado di comprovarlo

principio di responsabilizzazione o *accountability*

Principi e definizioni

AiFOS

Le categorie di dati

PERSONALI

Qualsiasi informazione riguardante una persona fisica identificata o identificabile, direttamente o indirettamente, con particolare riferimento a un identificativo come: il nome - un numero di identificazione - un dato relativo all'**ubicazione** - un **identificativo online** - uno o più **elementi caratteristici della sua identità** fisica, fisiologica, genetica, psichica, economica, culturale o sociale

CATEGORIE PARTICOLARI DI DATI PERSONALI

origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale; 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.

GENETICI

Relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica, forniscono informazioni univoche sulla sua fisiologia o sulla sua salute, e risultano in particolare dall'analisi di un suo campione biologico

BIOMETRICI

Ottenuti da un trattamento tecnico specifico e relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici

RELATIVI ALLA SALUTE

Attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute

RELATIVI A CONDANNE PENALI O REATI

Relativi alle condanne penali e ai reati o a connesse misure di sicurezza

AiFOS

TRATTAMENTO – le operazioni sui dati

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

Principi e definizioni

AiFOS

INTERESSATI – le operazioni sui dati

Chi sono o possono essere i soggetti interessati al trattamento ?

Tutti coloro che cedono i propri dati personali a un'entità, pubblica o privata nell'ambito di uno specifico rapporto con essa.

Cioè …

- I cittadini nei confronti delle istituzioni
- I clienti
- I dipendenti
- I malati
- Gli iscritti a un partito politico, a un'associazione o una fondazione
- I donatori di una ONLUS
- Gli utenti di un servizio pubblico
- Gli utilizzatori di una APP gratuita
- Gli intestatari di un conto corrente o di una polizza assicurativa
- Gli iscritti a un programma di fidelity card
- Gli alunni di un istituto scolastico
- Gli utilizzatori di un servizio di comunicazione elettronica
- Gli acquirenti di beni tramite un sito di commercio elettronico
- Gli intestatari di un contratto telefonico

NOI TUTTI!

AiFOS

FINALITA'

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

a) l'interessato ha espresso il **consenso** per una o più specifiche finalità;

b) il trattamento è necessario **all'esecuzione di un contratto** o all'esecuzione di misure precontrattuali adottate su richiesta;

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

AiFOS

Il Regolamento EU 679/2016

Questo sconosciuto…

proseguiamo….

Come si deve comportare l'Organizzazione

AiFOS

INFORMARE

Tutti i soggetti interessati devono conoscere

- **L'identità** e i dati di contatto del Titolare del trattamento e, se presente, del Responsabile della protezione dei dati personali
- Le **finalità**, la durata e le basi di legittimità del trattamento
- Gli eventuali destinatari dei loro dati personali
- In caso di **trasferimenti verso paesi terzi** o organizzazioni internazionali, dettagli in merito al luogo di trasferimento e all'esistenza di garanzie adeguate per la tutela dei loro diritti
- Le possibili conseguenze di un mancato conferimento dei dati personali
- L'eventuale utilizzo di strumenti di profilazione o l'esistenza di decisioni automatizzate che lo riguardano
- La possibilità di esercitare i **propri diritti** e la possibilità di proporre reclami

Come si deve comportare l'Organizzazione

AiFOS

Trattamenti basati sul consenso degli interessati

Il consenso raccolto ha valore se è:

- fornito liberamente
- specifico
- informato
- inequivocabile
- revocabile con la stessa facilità con la quale è concesso

Come si deve comportare l'Organizzazione

AiFOS

Registro dei trattamenti

- È tenuto in forma scritta, anche elettronica.
- Contiene le informazioni essenziali in merito ai dati personali custoditi dall'impresa e alle operazioni di trattamento effettuate sui dati personali, alle loro caratteristiche e alle entità coinvolte nel processo; racconta in che modo l'impresa elabora, protegge, archivia e cancella i dati.
- Deve essere esibito se richiesto dall'Autorità Garante
- Un Registro ben scritto, ben tenuto e mantenuto è il primo passo verso la conformità.
- L'obbligatorietà della sua redazione dipende dallo specifico contesto.

Come si deve comportare l'Organizzazione

AiFOS

Rapporti con terze parti e fornitori

Tutti coloro che:

- **trattano dati per conto del titolare del trattamento**
- **ricevono dati personali dal titolare del trattamento**
- **entrano in contatto con dati personali nell'erogazione di un contratto di servizio con il titolare del trattamento**

Devono

- essere opportunamente istruiti
- agire, se del caso, in virtù di un contratto o di un atto giuridico vincolante che stabilisca chiaramente compiti, responsabilità e confini del trattamento
- essere selezionati in virtù di competenze e caratteristiche possedute, sulla base del principio di responsabilizzazione del titolare

Come si deve comportare l'Organizzazione

AiFOS

Nomine (interne ed esterne)

- Ciascun Responsabile del Trattamento (entità fisica e giuridica diversa dal Titolare del Trattamento) deve essere formalmente nominato
- L'eventuale Responsabile della Protezione dei dati personali (**RPD o DPO**) – obbligatorio per tutti i soggetti pubblici e in alcuni casi particolari – deve essere formalmente nominato. Il suo nome deve essere comunicato all'Autorità Garante.

Altre figure interne

- Operano sotto l'autorità del Titolare secondo quanto prescritto dall'art. 29
- Possono essere una opportunità organizzativa per organizzazioni complesse
- Esiste la tematica degli amministratori di sistema che rispondono da un provvedimento specifico (che si pensa verrà mantenuto)

scegliere sempre adeguatamente

formare adeguatamente

Come si deve comportare l'Organizzazione

AiFOS

Misure tecnico – organizzative adeguate al contesto

Ogni specifica situazione richiede

l'implementazione di «*misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al* ***rischio*****»**

Esse possono includere

- **l'adozione di strumenti tecnici**
- **la revisione delle procedure esistenti, delle politiche o dei processi**
- **la modifica di alcune delle applicazioni IT utilizzate**
- **l'implementazione di nuovi processi**

Ogni decisione

richiede una valutazione preventiva e accurata dei

rischi connessi al trattamento di dati personali

Come si deve comportare l'Organizzazione

AiFOS

Al momento di determinare mezzi e modalità del trattamento, e tenendo conto di:

- stato dell'arte e costi di attuazione
- natura, ambito di applicazione, contesto e finalità del trattamento
- rischi derivanti dal trattamento e aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche

Sicurezza del Trattamento

il Titolare deve mettere in atto misure tecniche e organizzative per attuare in modo efficace i principi di protezione dei dati, quali la **pseudonimizzazione** o la **minimizzazione**, e **per integrare nel trattamento le necessarie garanzie** al fine di tutelare i diritti degli interessati

Privacy by design – Privacy by default

Ai fini della protezione dei dati fin dalla progettazione e per impostazione predefinita , il Titolare deve:

- **progettare servizi e prodotti** che **includono la protezione dei dati personali fin dall'inizio**
- prevedere misure adeguate per **garantire che siano trattati**, per impostazione predefinita, **solo i dati personali necessari** per ogni specifica finalità del trattamento: l' obbligo **vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità**
- fare in modo che i dati personali - per impostazione predefinita - **non siano resi accessibili a un numero indefinito** di persone fisiche

AiFOS

Violazioni e comunicazione

In caso di violazione dei dati personali, il **Titolare del Trattamento** notifica la violazione all'autorità di controllo competente senza ingiustificato ritardo e, 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.*

In presenza di un rischio elevato per i diritti e le libertà delle persone fisiche, la violazione deve essere **comunicata all'interessato** senza ingiustificato ritardo.

La comunicazione non è richiesta se:

- ai dati personali oggetto di violazione erano state applicate adeguate misure tecniche e organizzative di protezione – ad esempio la cifratura - destinate a rendere i dati personali incomprensibili a chiunque non fosse autorizzato ad accedervi
- a seguito della violazione e per i dati oggetto di data breach, sono state adottate misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati
- la comunicazione richiederebbe sforzi sproporzionati. In tal caso, è possibile effettuare una comunicazione pubblica tramite la quale si possono informare con uguale efficacia gli interessati.

Come si deve comportare l'Organizzazione

AiFOS

Una Organizzazione deve puntare sempre alla sua sopravvivenza

Questo implica che l'organizzazione deve effettuare ciclicamente e costantemente una propria analisi dei rischi

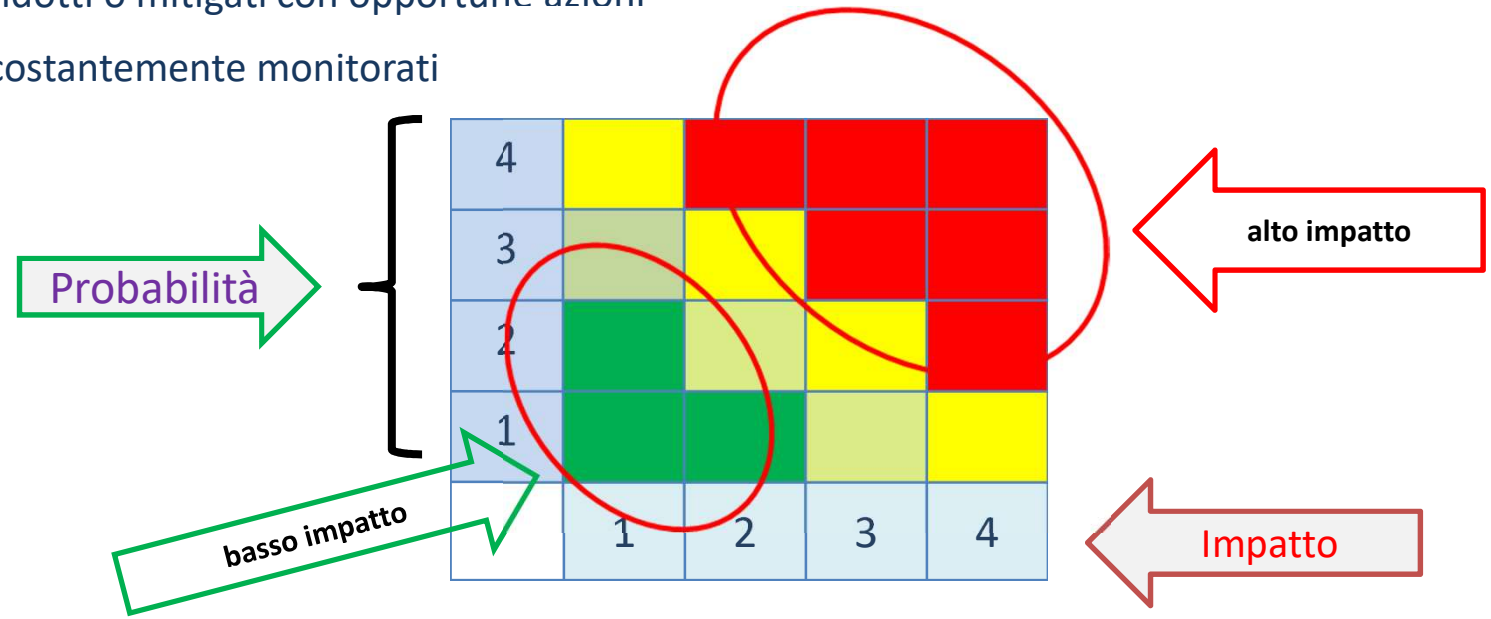
Come si deve comportare l'Organizzazione

AiFOS

Analizzare il rischio sui dati personali

I rischi connessi al trattamento dei dati personali devono essere:

- identificati
- descritti
- valutati
- ridotti o mitigati con opportune azioni
- costantemente monitorati



Come si deve comportare l'Organizzazione

AiFOS

Le principali minacce inerenti la protezione dati personali da analizzare

Accesso illegittimo ai dati

Modifica non prevista dei dati

Furto di dati

Vedi definizioni
ISO/IEC 29134:2017

AiFOS

Pianificazione e implementazione: il trattamento del rischio

Azioni preventive che hanno l'obiettivo di tenere sotto controllo un rischio

Accettazione Il rischio è ritenuto accettabile (è quantificato e si stanziano accantonamenti)	**Riduzione** Il rischio deve essere ridotto. Si intraprendono azioni per diminuire i danni o la probabilità	**Condivisione** Il rischio è condiviso con altri soggetti (delega/nomina/ suddivisione)
Trasferimento Il rischio è ceduto ad altri (polizze assicurative)	**Diversificazione** Si sceglie di aumentare il numero di *item* (es. portafogli finanziari) o di frammentare i dati per ridurre danni o probabilità	**Non assunzione** Il rischio è eliminato perché non accettabile (progetto non avviato)

Come si deve comportare l'Organizzazione

AiFOS

Privacy *by design & by default*

By default

- Predisporre misure tecniche o organizzative per garantire che per definizione e fin dalla raccolta, siano trattati per ciascun processo, solo i dati personali strettamente necessari al perseguimento della finalità specifica

By design

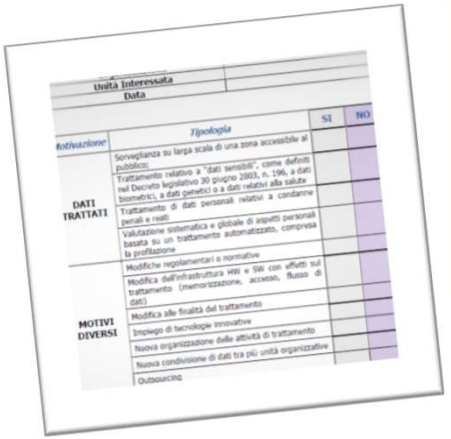
- Tenere in considerazione, fin dalla fase di progettazione di un nuovo servizio o prodotto, i rischi connessi al trattamento.
- Gestire i rischi emersi per minimizzarli e inglobare la privacy nei processi in modo preventivo e, per così dire, «nativo».

Come si deve comportare l'Organizzazione

Valutazione d'impatto sulla protezione dei dati personali – art. 35 (1)

Si effettua **prima di procedere** al trattamento e **quando un tipo di trattamento**, soprattutto se effettuato con l'ausilio di **nuove tecnologie**, può presentare **un rischio elevato per i diritti e le libertà delle persone fisiche**.

Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.


Unità Interessata
Data

Motivazione	Tipologia	SI	NO
DATI TRATTATI	Sorveglianza su larga scala di una zona accessibile al pubblico;		
	Trattamento relativo a "dati sensibili", come definiti nel Decreto legislativo 30 giugno 2003, n. 196, a dati biometrici, a dati genetici o a dati relativi alla salute		
	Trattamento di dati personali relativi a condanne penali e reati		
	Valutazione sistematica e globale di aspetti personali basata su un trattamento automatizzato, compresa la profilazione		
MOTIVI DIVERSI	Modifiche regolamentari o normative		
	Modifica dell'infrastruttura HW e SW con effetti sul trattamento (memorizzazione, accessi, flusso di dati)		
	Modifica alle finalità del trattamento		
	Impiego di tecnologie innovative		
	Nuova organizzazione delle attività di trattamento		
	Nuova condivisione di dati tra più unità organizzative		
	Outsourcing		

La DPIA (**D**ata **P**rotection **I**mpact **A**nalysis**) è sempre richiesta se:**

- **si effettua profilazione** e detta profilazione produce valutazione di aspetti della personalità che comportano **decisioni che possono avere effetti giuridici sugli Interessati;**
- l'oggetto del trattamento sono **dati biometrici o giudiziari;**
- si effettua **sorveglianza con strumenti ottico-elettronici.**

AiFOS

Indicazioni del WP29 (*Comitato Europeo Per La Protezione Dei Dati)* – caratteristiche della Data Protection Impact Analysis

Il WP29 per la DPIA:

- **l'obbligo** di condurre una DPIA vige per i **trattamenti in corso** che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche e per i quali siano intervenute variazioni dei rischi tenuto conto della natura, dell'ambito, del contesto e delle finalità dei trattamenti stessi a meno di non avere già una verifica preliminare dell'Autorità Garante;
- la DPIA dovrebbe essere condotta "**prima di procedere al trattamento**", per rendere le relative operazioni coerenti con i principi di protezione dei dati sin dalla fase di progettazione e per impostazione predefinita;
- la DPIA deve essere considerata uno strumento di ausilio nel processo decisionale relativo al trattamento;
- Il **TITOLARE è responsabile della corretta DPIA** (sentito il parere del RDP-DPO);
- è un **processo iterativo**.

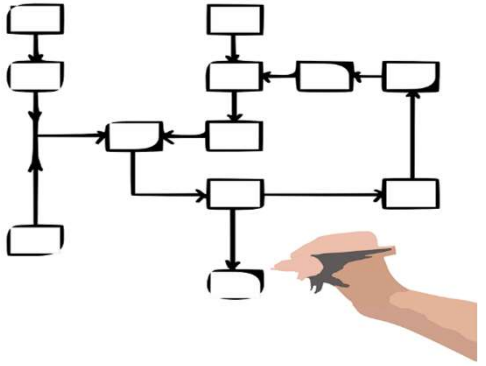
Come si deve comportare l'Organizzazione

AiFOS

Processi e procedure

L'organizzazione deve dotarsi, o adattare, di procedure relative a (a titolo di esempio non esaustivo):

- cancellazione dei dati personali
- gestione delle richieste degli interessati, inclusa la portabilità dei dati
- gestione delle violazioni per il tempestivo intervento e la notifica all'Autorità Garante
- modello di valutazione preliminare d'impatto (DPIA)
- gestione del consenso degli interessati
- conservazione delle evidenze
- gestione delle diverse versioni dei documenti
- individuazione di responsabilità
- formazione ed aggiornamento degli addetti



Come si deve comportare l'Organizzazione

AiFOS

Ulteriori punti di attenzione

- trasferimento di dati personali verso paesi non UE
- risorse dedicate alla protezione dei dati (umane ed economiche)
- opportunità di implementare e mantenere un sistema di gestione dei dati personali
- possibilità di aderire a Codici di Condotta di settore o di sottoporsi a specifica certificazione
- predisposizione del proprio Registro dei trattamenti – anche quando non dovesse essere un obbligo normativo
- inserimento dei rischi legati al trattamento dei dati personali nella mappatura dei rischi aziendali

Come si deve comportare l'Organizzazione

AiFOS

In estrema sintesi una Organizzazione deve (almeno):

- Determinare le **finalità** e le basi di **legittimità del trattamento**
- Determinare se si opera su «**dati raccolti**» o «**dati raccolti da altre organizzazioni**»
- Determinare la **posizione dei dati** (Italia, Europa, estero)
- Determinare i **soggetti coinvolti** nel trattamento sia interni sia esterni
- **Informare i propri interessati**
- Raccogliere gli eventuali **consensi** e gestirli
- Individuare i Trattamenti e annotarli (**Registro dei Trattamenti**)
- **Analizzare i rischi** cui sono sottoposti i dati affidati
- **Proteggere** adeguatamente i dati (digitali e cartacei) affidati
- Attivare procedure per rispondere prontamente alle **violazioni**
- …

Annotare tutto per dimostrare l'accountability

Azioni

AiFOS

Ma operativamente che vuol dire ?

- Individuazione del «ruolo» o dei «ruoli» svolti dall'organizzazione
- Individuazione delle basi giuridiche di legittimità del trattamento
- Predisposizione Registro dei Trattamenti
- Predisposizione informative per interessati esterni (clienti, associati)
- Predisposizione moduli di raccolta del consenso e gestirlo
- Predisposizione informative dipendenti e collaboratori
- Nomine: DPO – Responsabili – Amministratori di Sistema
- Revisione contratti con fornitori di prodotti o servizi con accesso ai dati personali per inserimento clausole di dettaglio, come richiesto dalla norma
- Revisione sito web (informativa, cookies policy)

Azioni

AiFOS

Cosa devono fare le imprese - 2/2

- Revisione e correzione dei processi interni
- Revisione delle procedure esistenti
- Predisposizione di un processo per la gestione delle violazioni con indicazioni procedurali (azioni e responsabilità)
- Predisposizione di un processo per la gestione dei diritti degli interessati con indicazioni procedurali (azioni e responsabilità)
- Processo di gestione dei documenti privacy
- Revisione IT: applicazioni, prodotti, rete, sicurezza, *cloud*
- Predisposizione di regolamenti interni
- Istruzione e formazione degli addetti
- Politiche di gestione e cancellazione dati (anche cartacei)

Conclusione

AiFOS

Lo sviluppo di consapevolezza è interesse delle imprese

Perché:

- favorisce la protezione di tutte le informazioni aziendali, non solo dei dati personali
- determina l'instaurarsi di comportamenti virtuosi, alla base del processo di miglioramento continuo
- rende i processi di cambiamento più agevoli e veloci
- facilita l'eliminazione di punti di debolezza «nascosti» e di possibili punti di accesso per violazioni

Formare e informare è uno dei principali doveri del titolare del trattamento

AiFOS

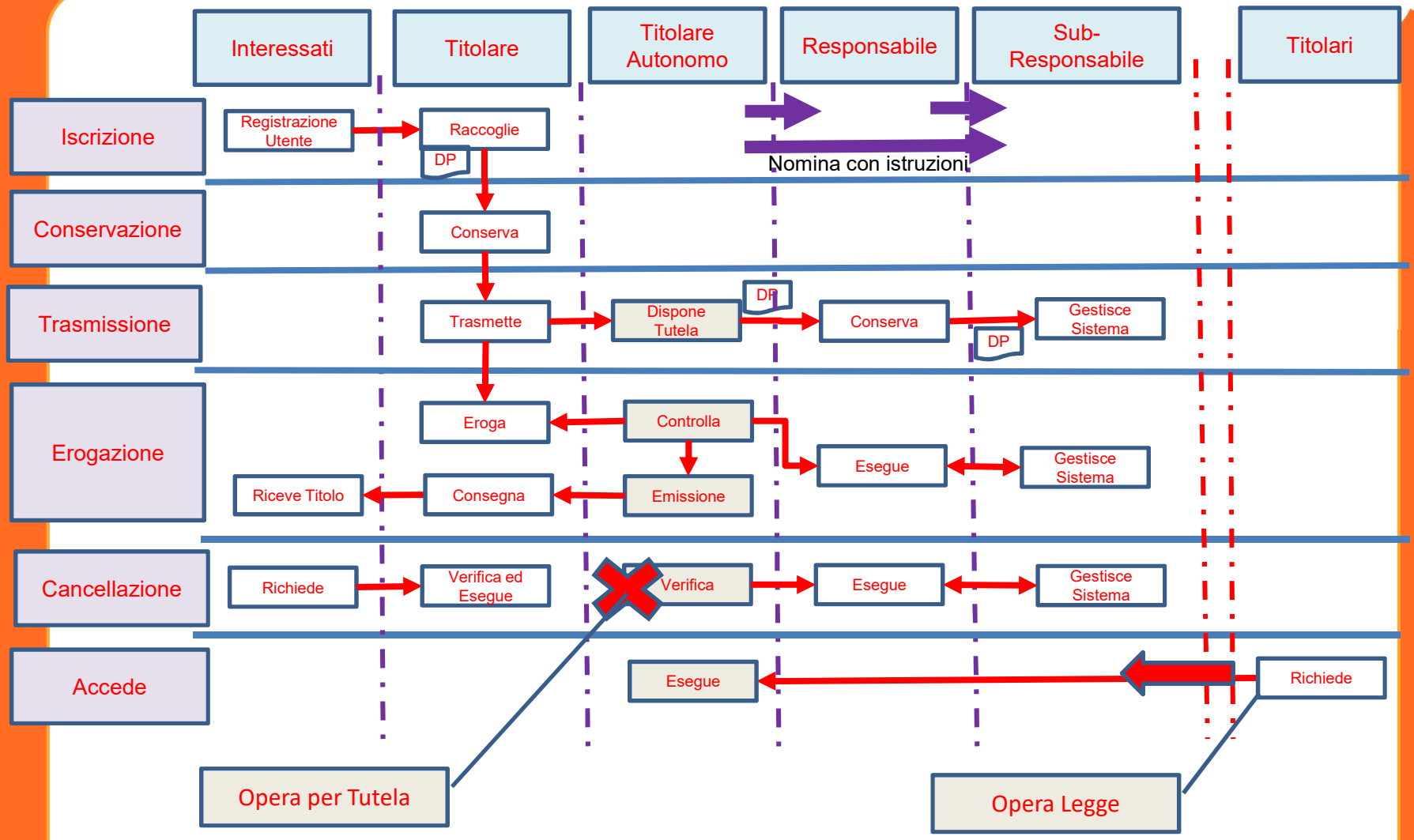
Il Regolamento EU 679/2016

Operativamente……

Tutti gli esempi illustrati non possono ritenersi esaustivi

Inseguite i dati ……

AiFOS



AiFOS

I contenuti dell’informativa (1)

1. Il **nome** e i **dati di contatto** del Titolare del Trattamento e del suo eventuale **Rappresentante**
2. I **dati di contatto** del **Responsabile della protezione dei dati**, ove applicabile
3. Le **finalità** e la **base giuridica del trattamento** cui sono destinati i dati personali
4. Gli **eventuali destinatari** o le categorie di destinatari dei dati personali
5. Se del caso, l’**intenzione** del Titolare **di trasferire i dati personali a un paese terzo o a un’organizzazione internazionale**: è necessario precisare il luogo di trasferimento e le garanzie adottate nonché le modalità attraverso le quali sia possibile per l’interessato ottenere una copia dei propri dati
6. Il **periodo di conservazione** dei dati personali oppure, se non è possibile, i criteri utilizzati per determinarlo

AiFOS

I contenuti dell'informativa (2)

7. L'**esistenza di diritti fondamentali** per ogni interessato e la possibilità di esercitarli
8. Il **diritto di revocare il consenso** in qualsiasi momento
9. Il **diritto di presentare reclamo** a un'autorità di controllo
10. L'esistenza di **obblighi legali o contrattuali** o di requisiti necessari per la conclusione di un contratto che determinano la necessità per l'interessato di comunicare i propri dati personali, **nonché le possibili conseguenze dalla mancata comunicazione**
11. L'esistenza **di un processo decisionale automatizzato, compresa la profilazione** e, almeno in tali casi, le informazioni sulla **logica utilizzata** e le **conseguenze previste** di tale trattamento per l'interessato

L’informativa – un esempio …. (1)

AiFOS

TITOLARE DEL TRATTAMENTO

Titolari del trattamento dei dati personali del sito www.THEsitodiprova.com è Sebastiano plutino– via Ettore 16 – 90148 CANICATTI’ - P.IVA 1444444444 .

Per qualunque informazione può contattare all’indirizzo email info@thesitodiprova.com .

ORIGINE DEI SUOI DATI E CATEGORIE DI DATI TRATTATI

I dati oggetto di trattamento sono quelli da Lei forniti al momento della compilazione delle maschere presenti sul sito per avere informazioni, ricevere materiale o per accordi precontrattuali. I dati raccolti sono nome, cognome e indirizzo email di contatto.

INFORMAZIONI RACCOLTE DURANTE LA NAVIGAZIONE NEL SITO - COOKIE

Per una descrizione estesa dei cookie si rimanda a quanto contenuto nella **Cookie Policy**. Sul sito sono presenti i cookie di sessione che agevolano la consultazione del sito e si cancellano alla fine del contatto, e Google Analytics configurato per raccogliere in maniera anonimizzata dati sulla consultazione delle pagine per statistiche aggregate che permettono l’analisi di alcuni aspetti della navigazione sul sito (ad esempio le pagine più visitate).

Tutti gli esempi illustrati non possono ritenersi esaustivi

L'informativa – un esempio …. (2)

AiFOS

FINALITÀ DEL TRATTAMENTO

Sitodiprova.com tratta i Suoi dati personali come sopra definiti e indicati per le finalità di seguito illustrate e secondo le basi di liceità richiamate nel RGPD e a fianco specificate.

a) **Per rispondere a specifiche richieste dei visitatori del sito** (RGPD, art. 6, comma 1, lett. b), e per il relativo invio di informazioni e/o materiale;

b) **Per il per il perseguimento del legittimo interesse del titolare** (RGPD, art. 6, comma 1, lett. f).
A titolo puramente esemplificativo e non esaustivo:

- la sicurezza e la salvaguardia dei propri sistemi informativi e del sito;
- l'analisi statistica delle visite effettuate e delle pagine più visitate;
- la gestione di eventuali contenziosi o controversie giudiziarie.

Thesitodiprovar.com non effettua profilazione.

Tutti gli esempi illustrati non possono ritenersi esaustivi

L’informativa – un esempio …. (3)

AiFOS

LUOGO DI TRATTAMENTO DEI DATI E MODALITÀ DI TRATTAMENTO

I suoi dati sono trattati nel territorio italiano. Tutte le operazioni – raccolta, elaborazione, consultazione, stampa, archiviazione, modifica, aggiornamento – potranno essere svolte su supporto cartaceo o per mezzo di strumenti elettronici.

COMUNICAZIONE DEI SUOI DATI A TERZI

The Project Player ha affidato i servizi di sviluppo e manutenzione del sito a un fornitore specializzato, appositamente nominato Responsabile del Trattamento; il sito e il dominio di posta utilizzato per la ricezione delle richieste dei visitatori e l’invio di informazioni sono gestiti in hosting da HOSTING S.p.A. all’interno del territorio dell’Unione Europea. I dati personali raccolti non sono diffusi ad altri soggetti.

PERIODO DI CONSERVAZIONE DEI DATI

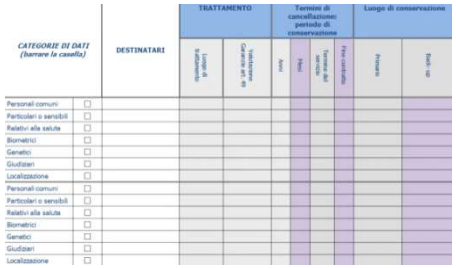
I dati raccolti per la finalità illustrata al precedente punto a) saranno conservati per lo scambio di informazioni e saranno cancellati al più tardi entro i 12 mesi dall’ultimo contatto con il Titolare.

Ricordarsi i diritti degli interessati

Tutti gli esempi illustrati non possono ritenersi esaustivi

AiFOS

Obblighi del Titolare



Il Registro del Titolare deve contenere:

- nome e contatti del Titolare, del suo Rappresentante e, se del caso, del Responsabile della protezione dei dati;
- le finalità del trattamento, inclusi gli eventuali legittimi interessi;
- la descrizione delle categorie di interessati;
- la descrizione delle categorie di dati;
- le categorie di eventuali destinatari, inclusi quelli collocati in paesi terzi (non UE);
- la documentazione delle garanzie adeguate per tutti i trasferimenti verso i paesi terzi che avvengono nelle situazioni descritte all'articolo 49;
- i termini di cancellazione dei dati personali;
- la descrizione generale delle misure di sicurezza tecnico-organizzative.

Il Registro dei Trattamenti …. (1)

AiFOS

TITOLARE DEL TRATTAMENTO		
NOME E COGNOME O RAGIONE SOCIALE Padenghe	COD. FISCALE / P.IVA 999999	INDIRIZZO E-MAIL padenghe@padenghe.it
RESPONSABILE DELLA PROTEZIONE DATI		
NOME E COGNOME O RAGIONE SOCIALE Al momento non c'è	COD. FISCALE / P.IVA ppppppppp	INDIRIZZO E-MAIL

E' utile aggiungere un documento su cui inserire le descrizioni delle tecniche utilizzate e le misure di protezione o di conformità *(privacy by design, privacy by default)*

Tutti gli esempi illustrati non possono ritenersi esaustivi

Il Registro dei Trattamenti …. (2)

AiFOS

Finalità: Esecuzione del contratto
Attività:
Funzione: Direzione

Categorie interessati	Basi del trattamento	Numero interessati
Clienti	Esecuzione contrattuale, Esecuzione contrattuale	Tra 250 e 1.000

Tipo trattamento	Operazioni sui dati	Luogo del trattamento	Luogo archiviazione	Luogo backup
Automatico e manuale	Raccolta – Modifica – Aggiornamento – Elaborazione, Consultazione e/o Stampa, Conservazione, Cancellazione	Italia	Italia	Italia

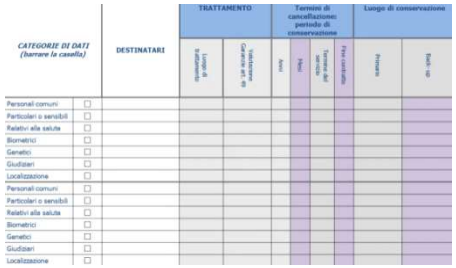
Categorie di dati	Origine dei dati	Termine di conservazione
Personali comuni	Acquisiti dall'interessato	10 anni

Destinatari dei dati	Ruolo	Categoria dati trasferiti	Luogo di trattamento
Enti di formazione	Altro Titolare	Personali comuni	Italia

Tutti gli esempi illustrati non possono ritenersi esaustivi

AiFOS

Obblighi dei Responsabili



Il Registro del Responsabile deve contenere:

- nome e contatto del Responsabile, di ogni titolare del trattamento per conto del quale il Responsabile agisce, del Rappresentante del Titolare o del Responsabile e, se del caso, del Responsabile della protezione dei dati;
- la descrizione delle categorie di trattamenti effettuati per conto di ogni Titolare;
- i trasferimenti verso i paesi terzi, compresa l'identificazione del paese terzo o dell'organizzazione internazionale;
- la documentazione delle garanzie adeguate per tutti i trasferimenti verso i paesi terzi che avvengono nelle situazioni descritte all'articolo 49;
- una descrizione generale delle misure di sicurezza tecnico-organizzative.

Il Registro dei Trattamenti – un esempio …. (1)

AiFOS

Dati del Responsabile del trattamento

Nome e cognome o ragione sociale *
lago di garda

Codice fiscale / P.IVA *
1111111

Indirizzo mail di contatto *
lago@lago.com

Responsabile della Protezione Dati

Se presente, inserire i dati del responsabile della Protezione Dati

Rappresentante del Responsabile del trattamento

Se presente, inserire i dati del Rappresentante del Responsabile del trattamento

Il trattamento è effettuato per conto del Titolare o di un Primo Responsabile?

- (●) Titolare
- ( ) Altro Responsabile

Dati del Titolare

Nome e cognome o ragione sociale *
padenghe

Codice fiscale / P.IVA *
99999999

Indirizzo mail di contatto *
padenghe@padenghe.c

Tutti gli esempi illustrati non possono ritenersi esaustivi

Il Registro dei Trattamenti – un esempio …. (2)

AiFOS

Finalità: Esecuzione del contratto
Attività:
Funzione: Direzione

Categorie interessati	Basi del trattamento	Numero interessati
Clienti	Esecuzione contrattuale, Esecuzione contrattuale	Tra 250 e 1.000

Tipo trattamento	Operazioni sui dati	Luogo del trattamento	Luogo archiviazione	Luogo backup
Automatico e manuale	Raccolta – Modifica – Aggiornamento – Elaborazione, Consultazione e/o Stampa, Conservazione, Cancellazione	Italia	Italia	Italia

Categorie di dati	Origine dei dati	Termine di conservazione
Personali comuni	Comunicati dal titolare	Durata del contratto aumentata di 30-60gg tempo tecnico)

Aggiungiamo finalità e basi del trattamento

Tutti gli esempi illustrati non possono ritenersi esaustivi

Una nomina a responsabile SPP – un esempio …. (1)

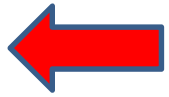
AiFOS

NOMINA A RESPONSABILE DEL TRATTAMENTO DEI DATI

XXXXXXX S.P.A., Società soggetta alla direzione e coordinamento di GRUPPO S.p.A., con sede legale in Lungotevere - 00193 Roma, iscritta al Registro Imprese di Roma - CF e n° iscriz. 999999999999, iscritta al R.E.A. di Roma al n° 99999999 - P.IVA n. 9999999999, in qualità di Titolare del Trattamento

PRESO ATTO CHE

- l'art. 28 del Reg. 679/2016, disciplina la nomina del Responsabile del Trattamento in capo ad un soggetto che per esperienza, capacità ed affidabilità fornisca idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza, per i trattamenti di dati personali, inclusi quelli di cui agli articoli 9 e 10 del Reg 679/2016;
- **SPP SRL** - Via Monte /A, 00112 - Roma (RM) - P.IVA/C.F. 0000000000 (di seguito **SPP s.r.l.**) – nell'ambito della Salute e sicurezza sul lavoro prevista dal Dlgs 81/2008 e s.m.i. è in possesso dei predetti requisiti di esperienza, capacità ed affidabilità e rispetta le disposizioni vigenti in materia di sicurezza del trattamento;
- **SPP s.r.l.** opera con propri sistemi informatici all'interno del territorio dell'UE e con professionisti di provata esperienza;



Tutti gli esempi illustrati non possono ritenersi esaustivi

Una nomina a responsabile SPP – un esempio …. (2)

AiFOS

CONSIDERATO CHE

- XXXXXXX S.p.A è Titolare del Trattamento dei dati anche personali dei propri dipendenti e di eventuali terzi (affini) per i trattamenti riportati di seguito:

Trattamento	• Gestione del servizio di prevenzione e protezione aziendale come previsto dal Dlgs 81/2008 (con particolare riferimento alla Titolo I Capo III Sez. III – art. 31-35 e correlati); • Gestione della sicurezza dei lavoratori; • Gestione della pianificazione delle visite mediche (effettuate dal medico competente); • Gestione di procedure e pratiche a seguito di eventuali infortuni o malattie professionali; • Gestione procedure per differenze di genere e di religione; • Gestione di particolari stati di riduzione della capacità lavorativa a seguito di disabilità temporanee o permanenti o di particolari stati (ad esempio: gestanti, puerpere, allattamento…); • Gestione della formazione (anche a scadenza) inerente salute e sicurezza sul lavoro; • Gestione della diffusione di informazione ai lavoratori; • Gestione delle risorse provenienti da subappalti E quant'altro inserito nelle competenze del Servizio di Prevenzione e protezione come definito dal Dlgs 81/2008.
Finalità perseguita	Gestione della salute e sicurezza del lavoratore e del processo lavorativo.
Base Giuridica	Esecuzione di contratto o di misure precontrattuali (art. 6.1.b del Reg EU 679/2016) Rispetto di quanto previsto dal Dlgs 81/2008 e s.m.i.;
Tipologia dei dati	Dati comuni, particolari, giudiziari ai sensi degli art. 9 e 10 del Reg.679/2016
Durata	Durata del rapporto di lavoro o del rapporto di collaborazione, maggiorata di 10 anni
Modalità	Automatica e manuale
Categorie di interessati	Dipendenti, e loro terzi correlati (affini), con qualunque tipo di contratto o consulenti. Dipendenti o assimilati di società terze che operano all'interno delle realtà produttiva.

- il Titolare del Trattamento necessita di supporto qualificato per le attività inerenti gli ambiti sopracitati;
- **SPP s.r.l.** eroga servizi diffusi nell'ambito della salute e sicurezza sul lavoro per organizzazioni e società clienti.

Tutti gli esempi illustrati non possono ritenersi esaustivi

Una nomina a responsabile SPP – un esempio …. (3)

AiFOS

NOMINA

SPP s.r.l. quale RESPONSABILE del TRATTAMENTO dei Dati comuni, particolari, giudiziari ai sensi degli art. 9 e 10 del Reg.679/2016 dei propri interessati (dipendenti, consulenti, subappaltatori) assegnandole i seguenti trattamenti:

Trattamento	• Gestione del servizio di prevenzione e protezione aziendale come previsto dal Dlgs 81/2008 (con particolare riferimento alla sezione III ed agli articoli correlati); • Gestione della sicurezza dei lavoratori; • Gestione della pianificazione delle visite mediche (effettuate dal medico competente); • Gestione di procedure e pratiche a seguito di eventuali infortuni o malattie professionali; • Gestione procedure per differenze di genere e di religione; • Gestione di particolari stati di riduzione della capacità lavorativa a seguito di disabilità temporanee o permanenti o di particolari stati (ad esempio: gestanti, puerpere, allattamento…); • Gestione della formazione (anche a scadenza) inerente salute e sicurezza sul lavoro; • Gestione della diffusione di informazione ai lavoratori; • Gestione delle risorse provenienti da subappalti E quant'altro inserito nelle competenze del Servizio di Prevenzione e Protezione come definito dal Dlgs 81/2008. Attraverso memorizzazione temporanea di dati, archiviazione di dati personali inseriti nel data base o in file system in qualunque formato, predisposizione dei file dati necessari per le trasmissioni telematiche ad enti esterni (Agenzia Entrate, INAIL, Organizzazioni datoriali, Enti di formazione, Assicurazioni, Associazioni Sindacali…) sempre connessi con la Salute e Sicurezza sul Lavoro di lavoro.
Finalità perseguita	Esecuzione di un contratto
Tipologia dei dati	Dati comuni, particolari, giudiziari ai sensi degli art. 9 e 10 del Reg.679/2016
Durata	Durata del contratto in essere con XXXXXXX S.p.A. maggiorata di 3 mesi (tempo tecnico di spostamento dei dati ad altro Responsabile)
Modalità	Automatica e manuale
Operazioni previste	Raccolta, Registrazione, Organizzazione, Strutturazione, Conservazione, Modifica, Estrazione, Consultazione, Elaborazione, Comunicazione, Cancellazione
Categorie di interessati	Dipendenti, e loro terzi correlati (affini), con qualunque tipo di contratto o di consulenti. Dipendenti o assimilati di società in subappalto che operano all'interno delle realtà produttiva.

Tutti gli esempi illustrati non possono ritenersi esaustivi

Una nomina a responsabile SPP – un esempio …. (4)

AiFOS

Al riguardo il **Titolare del Trattamento** dichiara di:

- avere erogato o di essere in procinto di erogare completa informativa a dipendenti e consulenti interessati, indicando espressamente **SPP s.r.l.** quale Responsabile nominato del Trattamento come sopra specificato;
- essere in possesso, ove necessario, del consenso alla gestione/trattamento dei dati da parte dei propri interessati, all'uopo manlevando **SPP s.r.l.**, da qualsivoglia responsabilità in merito alla gestione e all'eventuale aggiornamento degli stessi;
- avere una propria procedura di gestione delle violazioni sui dati personali; ogni eventuale violazione riscontrata sarà tempestivamente comunicata al Responsabile nominato per concordare l'adozione delle misure più opportune;
- affidare al Responsabile nominato le attività inerenti la corretta gestione della salute e sicurezza sul lavoro compresi i trattamenti necessari correlati per i dati comuni, particolari e giudiziari di tutti gli interessati.

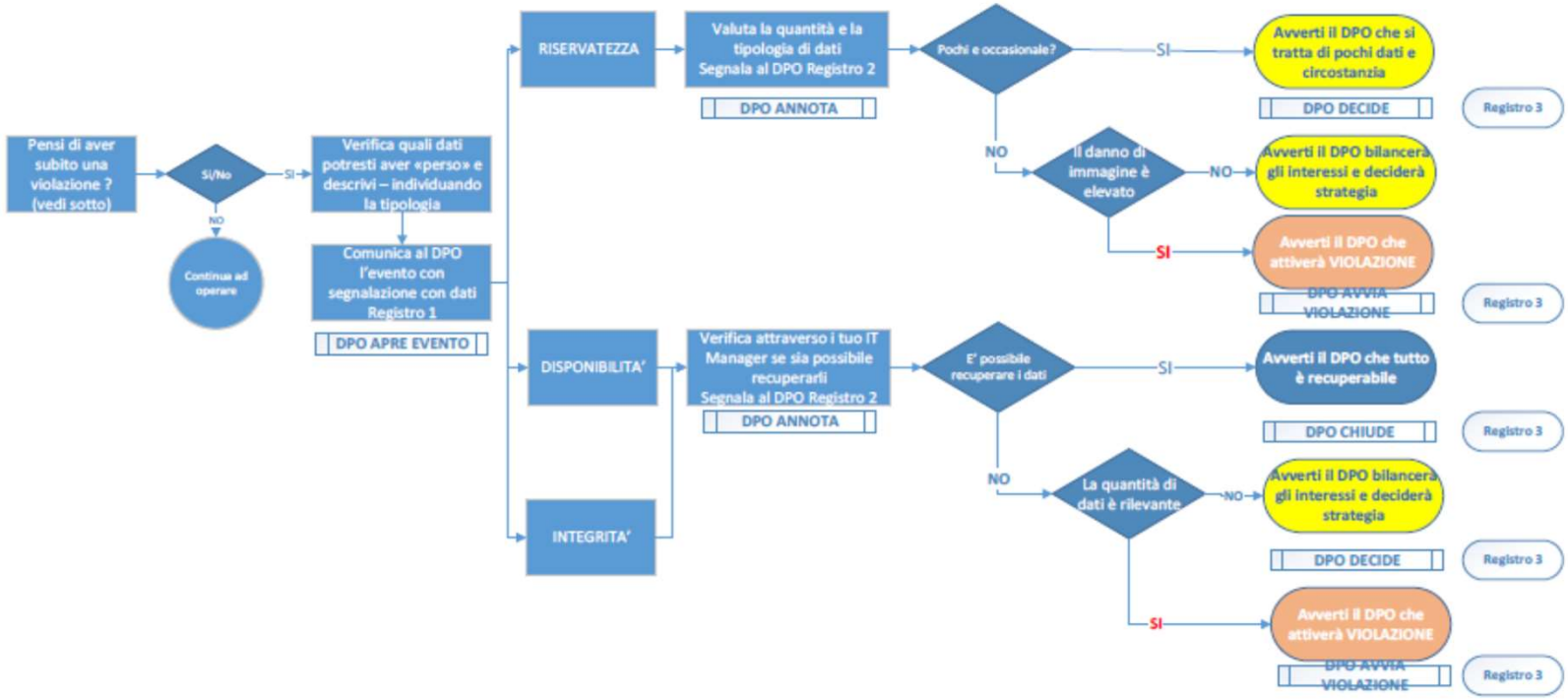
Il **Responsabile del Trattamento** da parte sua si impegna (ai sensi dell'art. 28 par. 3 Regolamento UE 2016/679) a:

- trattare i dati personali soltanto secondo le istruzioni del Titolare del Trattamento;
- effettuare le sole operazioni necessarie all'erogazione del servizio;
- trasferire i dati in paesi autorizzati dal diritto dell'Unione Europea fatti salvi i trasferimenti giuridicamente obbligati sempre preceduti da una richiesta di consenso esplicito, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
- garantire che le persone autorizzate al trattamento dei dati personali sotto l'autorità del Responsabile si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- garantire che le persone autorizzate al trattamento sotto l'autorità del Responsabile abbiano ricevuto esplicite istruzioni circa le modalità di trattamento di dati personali anche sensibili previste dal Reg. 679/2016;
- garantire che siano disponibili, a richiesta del titolare, elenchi delle attribuzioni di incarichi al personale che opera sotto l'autorità del Responsabile, ivi compresi gli amministratori di sistema;
- ricorrere ad altro responsabile del trattamento per le sole attività inerenti l'assistenza hardware e software e gli eventuali servizi di recovery fatti su piattaforme anche cloud conformi alla legislazione della Unione Europea, comunicandone gli estremi al Titolare e richiedendo ai fornitori identiche tutele;
- ricorrere ad altro responsabile o altro titolare del trattamento per gli interventi formativi, comunicandone gli estremi al titolare (in caso di ricorso a titolari autonomi comunicare al titolare le motivazioni giuridiche della scelta di titolari autonomi);

Tutti gli esempi illustrati non possono ritenersi esaustivi

Una procedura di gestione delle violazione – un esempio

AiFOS



Tutti gli esempi illustrati non possono ritenersi esaustivi

amo finito….

AiFOS

Sviluppare una prima versione dei documenti previsti dal Regolamento permette di dimostrare di voler procedere verso la conformità

Ma non finisce qui…

la conformità va coltivata perché diventi un valore e un investimento di cui pregiarsi e farne un vanto

… amo veramente finito….

AiFOS

Grazie per attenzione e pazienza!!!

DISCLAIMER

AiFOS

UTILIZZO DELLE SLIDE

Il materiale utilizzato per la trattazione degli argomenti affrontati nel corso è propedeutico alla attività di formazione e costituisce una mera esemplificazione delle materie trattate.

Nessuna responsabilità legata a una decisione assunta sulla base delle informazioni qui contenute potrà, quindi, essere attribuita ai relatori o ad AiFOS.

È espressamente vietata la diffusione, anche parziale, del materiale a terzi nonché l'utilizzo dello stesso per qualsiasi scopo commerciale e/o di lucro.

Grazie per l'attenzione!

AiFOS
Associazione Italiana Formatori ed Operatori della Sicurezza sul Lavoro