NUCLEO SPECIALE TUTELA PRIVACY E FRODI TECNOLOGICHE

LA COMPLIANCE DEI SITI INTERNET AZIENDALI

Torino, 20 novembre 2023

Relatore: Ten. Col. Celeste Enza D'Ignazio

NUCLEO SPECIALE TUTELA PRIVACY E FRODI TECNOLOGICHE

N.S.T.P.F.T.

GRUPPO PRIVACY

DIPENDENZA GERARCHICA

COMANDO REPARTI SPECIALI

AUTORITÀ DI RIFERIMENTO

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NUCLEO SPECIALE TUTELA PRIVACY E FRODI TECNOLOGICHE

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

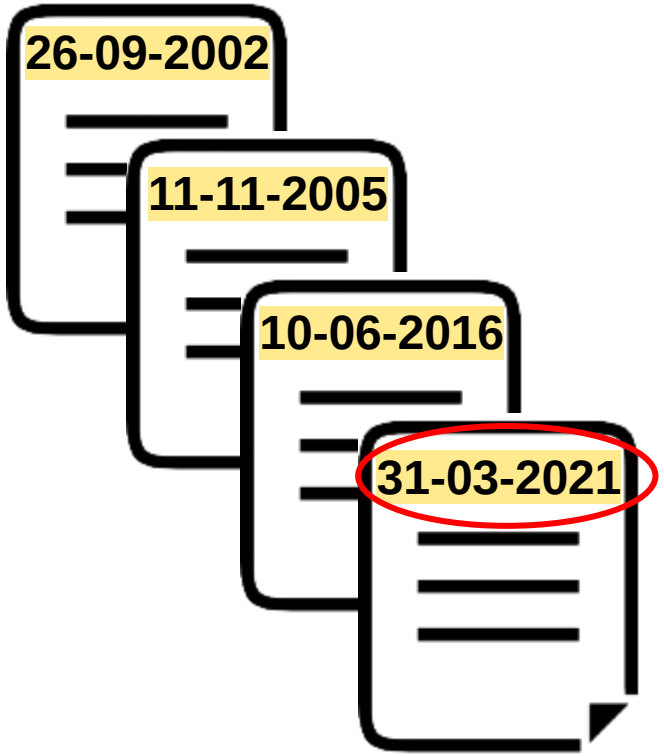
PROTOCOLLO D'INTESA
RELATIVO AI RAPPORTI DI COLLABORAZIONE TRA
IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI
E
LA GUARDIA DI FINANZA

Il Garante per la protezione dei dati personali (di seguito, anche "il Garante") e la Guardia di Finanza (di seguito, anche "il Corpo");

CONSIDERATO che il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, conferisce al Garante, in qualità di autorità di controllo, specifici poteri (art. 58) tra i quali pregnanti potestà di indagine che prevedono di:

- **Reperimento** di **dati e informazioni** da segnalare all'Autorità
- Esecuzione di **attività delegata** dell'Autorità Garante – **verifiche *on-line***
- Partecipazione ad **ispezioni congiunte** con l'Autorità Garante nonché ad **operazioni congiunte** con le Autorità di controllo di altri Stati membri (art. 62 GDPR)
- Sviluppo di **attività progettuali** in sinergia con i **Reparti territoriali del Corpo**
- **Sub-delega** di attività ai Reparti del Corpo dislocati sul territorio
- Gestione dei **rapporti con l'Autorità Garante**

AGGIORNAMENTO PROTOCOLLO D'INTESA



L'**art. 3** del D.Lgs. n. 68/2001 "Adeguamento dei compiti del Corpo della Guardia di finanza" (in attuazione dei principi direttivi della legge n. 78/2000) ha espressamente previsto la **collaborazione** della Guardia di Finanza - quale Polizia economico/finanziaria - con le Autorità Indipendenti.

BASE NORMATIVA DELL'ATTIVITA' ISPETTIVA

Art. 58 GDPR

a) **ingiungere** al titolare del trattamento e al responsabile del trattamento e, ove applicabile, al rappresentante del titolare del trattamento o del responsabile del trattamento, di **fornirle ogni informazione** di cui necessiti per l'esecuzione dei suoi compiti.

e) ottenere, dal titolare del trattamento o dal responsabile del trattamento, **l'accesso a tutti i dati** personali e a tutte le informazioni necessarie per l'esecuzione dei suoi compiti.

f) ottenere **accesso a tutti i locali** del titolare del trattamento e del responsabile del trattamento, compresi tutti gli **strumenti** e **mezzi** di trattamento dei dati, in conformità con il diritto dell'Unione o il diritto processuale degli Stati membri.

Art. 157 Codice Privacy

1. Nell'ambito dei poteri di cui all'articolo 58 del Regolamento, e per l'espletamento dei propri compiti, il Garante puo' richiedere al titolare, al responsabile, al rappresentante del titolare o del responsabile, all'interessato o anche a terzi di **fornire informazioni e di esibire documenti** anche con riferimento al contenuto di banche di dati.

Art. 158 Codice Privacy

1. Il Garante può **disporre accessi a banche di dati, archivi o altre ispezioni e verifiche** nei luoghi ove si svolge il trattamento o nei quali occorre effettuare rilevazioni comunque utili al controllo del rispetto della disciplina in materia di trattamento dei dati personali.
2. I controlli di cui al comma 1, nonché quelli effettuati ai sensi dell'articolo 62 del Regolamento, sono eseguiti da personale dell'Ufficio, con la partecipazione, se del caso, di componenti o personale di autorità di controllo di altri Stati membri dell'Unione europea.
3. **Il Garante si avvale anche, ove necessario, della collaborazione di altri organi dello Stato per lo svolgimento dei suoi compiti istituzionali.**
4. Gli accertamenti di cui ai commi 1 e 2, se svolti in un'**abitazione** o in un **altro luogo di privata dimora** o nelle relative appartenenze, sono effettuati con l'**assenso informato** del titolare o del responsabile, **oppure previa autorizzazione del presidente del tribunale** competente per territorio in relazione al luogo dell'accertamento, il quale provvede con decreto motivato senza ritardo, al più tardi entro tre giorni dal ricevimento della richiesta del Garante quando e' documentata l'indifferibilità dell'accertamento.

Art. 159 Codice Privacy

1. 1. Il personale operante, munito di documento di riconoscimento, …omissis… Nel procedere a rilievi e ad operazioni tecniche può altresì estrarre copia di ogni atto, dato e documento, anche a campione e su supporto informatico o per via telematica. Degli accertamenti è redatto sommario verbale nel quale sono annotate anche le eventuali dichiarazioni dei presenti.

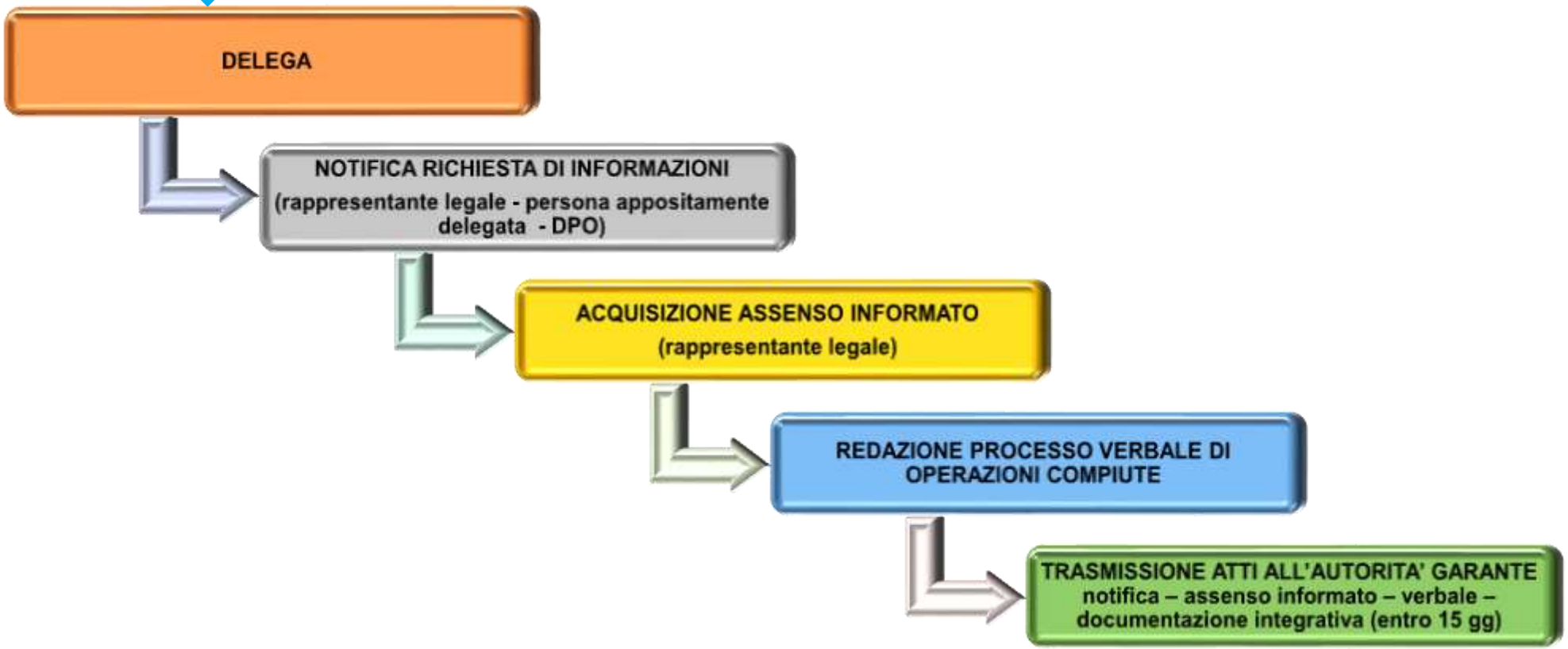
…omissis…

6. Quando emergono **indizi di reato** si osserva la disposizione di cui all'**art. 220 delle norme di attuazione**, di coordinamento e transitorie del codice di procedura penale…

…omissis…

L'ATTIVITA' ISPETTIVA: come si svolge?

ARTICOLO 58, COMMA 1, LETT. A) ED E) GDPR
+
ARTICOLI 157 E 158 CODICE PRIVACY



L'impresa "F.O.R.T.E." è…

- ***FAIR***
- ***ORIENTED***
- ***RESILIENT***
- ***TRUSTABLE***
- ***ENTERPRISE***

COMPLIANCE

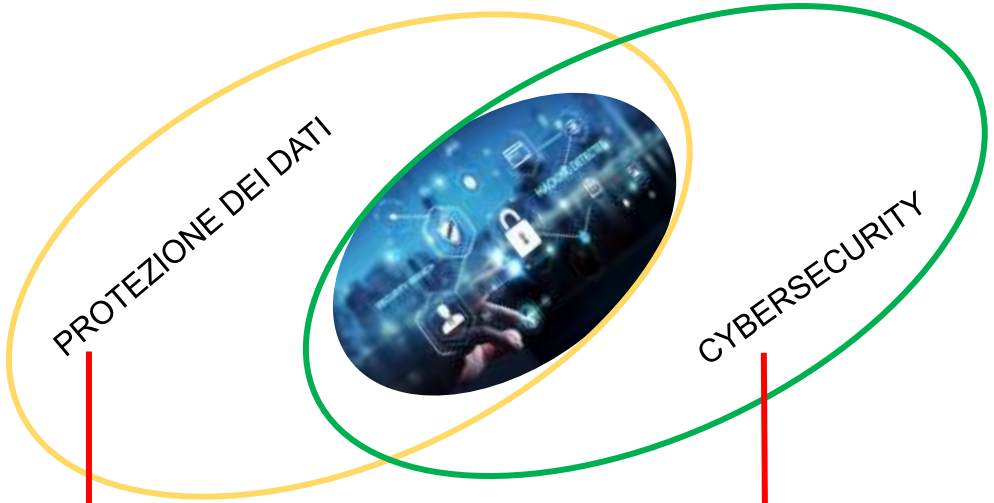
- sicurezza del lavoro
- tutela ambientale
- qualità gestionale
- anticorruzione e prevenzione dei reati
- **sicurezza informatica**
- **protezione dei dati**

→ COMPLIANCE PRIVACY →

COMPLIANCE PRIVACY nei siti web

Anche attraverso il sito web devono essere garantiti tutti i **diritti** e rispettati tutti i **principi** del GDPR.

NON esiste PROTEZIONE DEI DATI senza CYBERSECURITY
NON esiste CYBERSECURITY senza PROTEZIONE DEI DATI



tutela le persone dall'ORGANIZZAZIONE

Tutela le organizzazioni dalle PERSONE

è la prassi di **proteggere i sistemi, le reti e i programmi** dagli **attacchi digitali** solitamente finalizzati a:
- accesso/trasformazione/distrazione di informazioni sensibili;
- distorsione di denaro dagli utenti;
- interruzione di normali processi di lavoro.

NUCLEO SPECIALE TUTELA PRIVACY E FRODI TECNOLOGICHE

VERIFICHE **FRONT END**

PROTOCOLLO DI TRASMISSIONE SICURA

https://www.xyz.it/

2

SIMULAZIONE VERIFICA NEWSLETTER

- screenshot
- consenso implicito all'invio della richiesta
- verifica ricezione email contenente il *link* di conferma dell'iscrizione

1

SIMULAZIONI VERIFICHE COOKIE

- screenshot
- comando X
- scroll
- comandi OK e ACCETTA TUTTI
- nessun opt-in preimpostato
- reiterazione richiesta consensi

Linee guida cookie e altri strumenti di tracciamento 10 giugno 2021

ISCRIVITI ALLA NEWSLETTER

email

Informativa privacy

INVIA

REGISTRATI

nome *cognome*

città *indirizzo*

email *telefono*

Informativa privacy

acconsento al marketing

acconsento alla profilazione

INVIA

CONTATTI

nome

cognome

email

testo

Informativa privacy

INVIA

… … … banner cookie utilizzati … … … – **cookie policy** –

X

v tecnici ☐ terze parti ☐ profilazione OK ACCETTA TUTTI

3

SIMULAZIONE VERIFICA REGISTRAZIONE

- screenshot
- campi obbligatori
- consensi liberi e non pre-flaggati
- verifica ricezione email contenente il *link* di conferma della registrazione

VERIFICA E DOWNLOAD INFORMATIVE

4

SIMULAZIONE VERIFICA CONTATTI

- screenshot
- campi obbligatori

1 COOKIE E ALTRI STRUMENTI DI TRACCIAMENTO

CONSIDERANDO 30 - Le persone fisiche possono essere associate a identificativi *online* prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP**,** marcatori temporanei (***cookies***) o identificativi di altro tipo, quali i *tag* di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare, se combinate con identificativi univoci e altre informazioni ricevute dai *server*, possono essere utilizzate per creare profili delle persone fisiche e identificarle.

LINEE GUIDA COOKIE E ALTRI STRUMENTI DI TRACCIAMENTO - 10 giugno 2021

Tra le regole da rispettare e oggetto di verifica, i titolari dei siti *web* devono rendere un'informativa sull'utilizzo dei *cookies* avente un linguaggio semplice ed accessibile, *multilayer*, cioè dislocata su più livelli o anche resa tramite più canali e modalità (cosiddetto *multichannel*), ad esempio con il ricorso a *pop-up* informativi, interazioni vocali, assistenti virtuali, contatto telefono, *chatbot*, ecc.

Se si utilizzano solo ***cookie* tecnici**, la relativa **informazione può essere collocata in *home page*** o nell'**informativa generale del sito *web***.

Se si trattano anche altri ***cookie* «non tecnici»,** è indicato l'utilizzo di *banner* a comparsa immediata e di adeguate dimensioni che contengano:

- ❑ un **comando** (ad esempio, una **X** in alto a destra) per **chiudere il *banner* senza prestare il consenso** all'uso dei *cookie* o delle altre tecniche di profilazione mantenendo, così, le impostazioni di *default* che dunque, appunto per impostazione predefinita, non ne consentano l'impiego;
- ❑ l'indicazione che il sito utilizza *cookie* tecnici e se del caso, previo **consenso dell'utente**, ***cookie* di profilazione** indicando le relative finalità (**informativa breve**);
- ❑ il *link* alla ***privacy policy*** contenente **l'informativa completa**, inclusi gli eventuali altri soggetti destinatari dei dati personali, i tempi di conservazione dei dati e le modalità per esercitare i diritti di cui al Regolamento;
- ❑ un comando per accettare tutti i *cookie*;
- ❑ il *link* ad un'altra area nella quale poter scegliere in modo analitico le funzionalità, le **terze parti** e i *cookie* che si vogliono installare e, tramite due ulteriori comandi, poter modificare le scelte già fatte, prestando il consenso all'impiego di tutti i *cookie* se non dato in precedenza o revocandolo, anche in unica soluzione, se già espresso.

Lo ***scrolling* non** è ritenuto uno strumento adatto alla raccolta di un idoneo **consenso**, salva la sola ipotesi in cui venga inserito in un **processo più articolato**, nel quale l'utente sia in grado di generare un evento, registrabile e documentabile presso il *server* del sito, che possa essere qualificato come azione positiva idonea a manifestare in maniera inequivoca la volontà di prestare un consenso al trattamento.

2 NEWSLETTER

Una ***newsletter*** è un messaggio inviato via *email* in modo ricorrente ad una lista di contatti per tenerli aggiornati.

Qualora l'utente voglia, pertanto, essere aggiornato via email sulle novità di un sito *internet*, inserisce e inoltra tramite il ***form* dedicato** il proprio indirizzo di posta elettronica.

Quando il ***form* è specifico** per la finalità di *newsletter* **non** sarà necessario che l'utente rilasci il **consenso**, in quanto quest'ultimo è implicito nell'invio dell'indirizzo di posta elettronica per il servizio richiesto (**art. 6, par. 1, lett. b) del Regolamento UE 2016/679**).

Diversamente, quandunque il servizio di *newsletter* sia riportato quale **finalità ulteriore** rispetto a quella per la quale viene fornita l'email dall'utente (es.: "***form* contatti**" che prevede anche l'invio della *newsletter* nei confronti degli utenti che richiedono informazioni), deve essere prevista un'**apposita formula di consenso** e la spunta del relativo *check-box*, ai sensi dell'**art. 6, par. 1, lett. a) del Regolamento UE 2016/679** .

In entrambi i casi il titolare del sito *internet* è obbligato ad **informare** l'utente del trattamento dei dati personali effettuato per fornire il servizio di *newsletter*, ai sensi dell'**art. 13 del Regolamento UE 2016/679**, facendo particolare attenzione alle indicazioni sulle modalità di disiscrizione (**art. 7, par. 3 del Regolamento UE 2016/679**). Solitamente in calce alle *newsletter* è riportato il ***link "disclaimer"*** per disiscriversi dal servizio.

3 REGISTRAZIONE

Un **qualunque sito *internet***, anche un c.d. "**sito vetrina**" (non avente *form* di raccolta dati degli utenti), **tratta i dati personali di chi lo visita**, desumibili dall'**indirizzo IP** (*Internet Protocol*), quest'ultimo definito quale "*serie di numeri assegnata a ogni dispositivo connesso a una rete di computer o a Internet*". Detta informazione unitamente agli **altri elementi rilevati visitando le diverse pagine *web* di un sito *internet*** (es.: i nomi a dominio dei *computer* utilizzati dagli utenti che si connettono al sito, gli indirizzi in notazione URI - *Uniform Resource Identifier* - delle risorse richieste, l'orario della richiesta, il metodo utilizzato nel sottoporre la richiesta al *server*, la dimensione del file ottenuto in risposta, il codice numerico indicante lo stato della risposta data dal *server* - buon fine, errore, ecc. - ed altri parametri relativi al sistema operativo e all'ambiente informatico dell'utente) fa parte dei cc.dd. "**dati di navigazione**".

Non tutti i siti *internet* raccolgono e, quindi, **conservano i citati dati**; è **facoltà del gestore del sito *web* conservare** o meno dette **informazioni**. Chi conserva dette informazioni lo fa generalmente per un tempo determinato e per lo scopo di poter eventualmente risalire ad utenti che potrebbero essere oggetto di indagine da parte dell'Autorità Giudiziaria (pensiamo, per esempio, ai siti *web* dedicati a "giochi e scommesse" dove potrebbero perpetrarsi reati di riciclaggio).

In ogni caso il titolare del sito *internet* è obbligato ad **informare** l'utente del trattamento dei dati di navigazione effettuato, ai sensi dell'**art. 13 del Regolamento UE 2016/679**, facendo particolare attenzione alle **basi giuridiche**, alle **finalità** e ai **tempi di conservazione** dei dati e al principio di **minimizzazione** dei dati (**art. 5, par. 1, lett. c) del Regolamento UE 2016/679**).

Al contrario dei siti *internet* cc.dd. "vetrina", i siti di "***e commerce***" nascono con la previsione di raccogliere dati personali. L'obiettivo di chi si avvale di detti siti *web* è, infatti, quello di procedere alla vendita di prodotti e servizi. Per tale scopo è necessario che il titolare del sito *internet* acquisisca dati personali dell'utente al fine di vendere tramite pagamenti *on line* e di recapitare i prodotti a casa dell'utente.

La mole di dati personali utili a tale scopo comporta una **maggiore attenzione** in materia di protezione dei dati personali - già dalla fase di **progettazione** del sito *web* (**art. 25 Regolamento UE 2016/679**) - con particolare riguardo al principio di **minimizzazione** dei dati (**art. 5, par. 1, lett. c) del Regolamento UE 2016/679**).

Il titolare del sito *internet* è obbligato ad **informare** l'utente del trattamento dei dati personali effettuato per la vendita dei prodotti e dei servizi, ai sensi dell'**art. 13 del Regolamento UE 2016/679**, facendo particolare attenzione alla scelta dei **soggetti terzi**, di cui si potrebbe avvalere per rendere i servizi o per fornire i prodotti, e alla designazione, quali **responsabili** del trattamento, da formulargli ai sensi dell'**art. 28 del Regolamento UE 2016/679**.

4 CONTATTI

Quando si pensa alla raccolta dei dati degli utenti di un sito *web* per una richiesta di contatto si fa generalmente riferimento ad un ***form* di raccolta dati**, che prevede, il più delle volte, l'inserimento "**obbligatorio**" del nome e cognome, del numero di telefono e dell'indirizzo *email* dell'utente e il "testo" della richiesta. Il nome ed il cognome servono per individuare il richiedente, il numero di telefono per contattarlo direttamente ed evadere la richiesta, magari a seguito di alcune integrazioni e/o delucidazioni necessarie e da acquisire dal richiedente stesso, l'indirizzo *email* per fornire una risposta alla richiesta. L'obbligatorietà dell'inserimento di alcuni o di tutti i dati personali previsti dai campi del *form* in parola sarà dettata dalla **valutazione che farà preventivamente il titolare** sulla base delle esigenze dallo stesso ravvisate per rispondere alla richiesta di contatto.

Anche in questo caso il titolare del sito *internet* è obbligato ad **informare** l'utente del trattamento dei dati personali effettuato per evadere le richieste di contatto, ai sensi dell'**art. 13 del Regolamento UE 2016/679**, facendo particolare attenzione ai **tempi di conservazione** e al principio di **minimizzazione** dei dati (**art. 5, par. 1, lett. c) del Regolamento UE 2016/679**).

Attenzione! I dati personali raccolti per detta finalità non devono essere conservati né tanto meno utilizzati per attività di *telemarketing/smsmarketing* e/o *emailmarketing*. In questi casi il titolare è obbligato a **specificare nell'informativa le ulteriori finalità** del trattamento e ad acquisire, con apposita **formula di consenso** e spunta del relativo *check-box*, la volontà dell'utente a ricevere pubblicità tramite telefono e *email*, ai sensi dell'**art. 6, par. 1, lett. a) del Regolamento UE 2016/679**. Il titolare deve essere in grado di "**dimostrare**" il consenso da parte del titolare, ai sensi dell'**art. 7, par. 1, lett. a) del Regolamento UE 2016/679**, e predisporrà procedure tecniche per documentarne l'espressione o anche se di diniego da parte dell'interessato.

Inoltre, se ragioniamo sui possibili meccanismi di funzionamento dei *form* di raccolta dati, ci accorgiamo che, normalmente, cliccando sul tasto "invia", il sistema genera un'*email* avente come mittente l'indirizzo di posta elettronica associato al sito *internet*, come destinatario la casella di posta elettronica del titolare dello stesso sito *web* e per contenuto le informazioni inserite dall'utente. Da ciò potremmo considerare che il trattamento di dati personali che viene effettuato dal titolare del sito *internet* con un form di raccolta di dati personali per una richiesta di contatto è al pari di una richiesta di contatto pervenuta rispetto alla classica indicazione "**Per info e contatti scrivere a** XXX@dominio.it". In questo caso l'utente fornirà al titolare del sito *web* il proprio indirizzo *email* (necessario per inviare la richiesta di contatto) nonché ulteriori informazioni e dati personali che deciderà di inserire nella richiesta (es.: nome, cognome, telefono, ecc.). Anche in questo caso sono obbligatori gli adempimenti di cui sopra.

NUCLEO SPECIALE TUTELA PRIVACY E FRODI TECNOLOGICHE

VERIFICHE BACK END

5 AUTORIZZATI AL TRATTAMENTO

Art. 29 GDPR

- nomine
- partecipazione a corsi in materia di privacy e cybersecurity
- simulazione evento phishing
- verifiche periodiche sulle attività di trattamento svolte

www.xyz.it

1 *flusso*

Database sito web

query

flusso

flusso

flusso

2 ANALISI DEL RISCHIO/DPIA

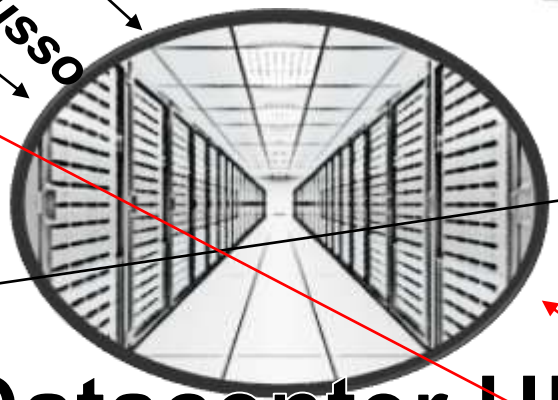
Art. 35 GDPR

3 AdS

- nomina
- verifica autenticazione
- estrazione file di log - tipologia – tempi di conservazione – immodificabilità
- …

4 *query*

- tipologia dati
- quantità di informazioni
- tempi di conservazione
- consensi
- blacklist
- gestione diritti
- utenti abilitati
- nomine autorizzati
- …



Datacenter UE

8 Datacenter EXTRA-UE

Trasferimento dati sulla base di una decisione di adeguatezza

Art. 45 GDPR

6 Misure di sicurezza

Art. 32 GDPR

7 DATA BREACH

Notifica di una violazione dei dati personali all'autorità di controllo

Art. 33 GDPR

Convegno Associazione ICT Dottori Commercialisti

TaxLawPlanet Webinar

1 DATABASE E DATACENTER UE

ARTICOLO 4 – DEFINIZIONI

Ai fini del Regolamento UE 2016/679 s'intende per:

6) «**archivio**» qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia **centralizzato**, **decentralizzato** o **ripartito** in modo funzionale o geografico;

8) «**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.

ARTICOLO 28 - RESPONSABILE DEL TRATTAMENTO

1. Qualora un trattamento debba essere effettuato **per conto del titolare del trattamento**, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto **misure tecniche e organizzative adeguate** in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

2. Il responsabile del trattamento non ricorre a un **altro responsabile** senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

3. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un **contratto** o da **altro atto giuridico** a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

2 ANALISI DEL RISCHIO/DPIA

Articolo 35 - Valutazione d'impatto sulla protezione dei dati

1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un **rischio elevato per i diritti e le libertà delle persone fisiche**, il titolare del trattamento effettua, **prima di procedere al trattamento**, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

2. Il **titolare del trattamento**, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il **responsabile della protezione dei dati**, qualora ne sia designato uno.

3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:
a) una **valutazione sistematica e globale** di aspetti personali relativi a persone fisiche, basata su un **trattamento automatizzato**, compresa la **profilazione**, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
b) il **trattamento, su larga scala, di categorie particolari** di dati personali di cui all'articolo 9, paragrafo 1, o di **dati relativi a condanne penali** e a reati di cui all'articolo 10;
c) la **sorveglianza sistematica su larga scala** di una zona accessibile al pubblico.

*__Linee guida sulla valutazione d'impatto sulla protezione dei dati (DPIA)__ e determinare se il trattamento è "suscettibile di comportare un rischio elevato" ai fini del Regolamento 2016/679, wp248rev.01

3 AMMINISTRATORE DI SISTEMA

Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 [doc. web n. 1577499]

Con la definizione di "**amministratore di sistema**" si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti.
Gli amministratori di sistema così ampiamente individuati, **pur non essendo preposti ordinariamente a operazioni che implicano una comprensione del dominio applicativo** (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), nelle loro consuete attività sono, in molti casi, concretamente "responsabili" di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati.
Attività tecniche quali il salvataggio dei dati (*backup/recovery*), l´organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione *hardware* comportano infatti, in molti casi, un´effettiva **capacità di azione su informazioni che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali**; ciò, anche quando l´amministratore non consulti "in chiaro" le informazioni medesime.
Valutazione delle caratteristiche soggettive: l´attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione dell´esperienza, della capacità e dell´affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza.
Designazioni individuali: la designazione quale amministratore di sistema deve essere in ogni caso individuale e recare l´elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.
Elenco degli amministratori di sistema: gli estremi identificativi delle persone fisiche amministratori di sistema, con **l´elenco delle funzioni ad essi attribuite**, devono essere riportati in un **documento interno da mantenere aggiornato** e disponibile in caso di accertamenti anche da parte del Garante.
Nel caso di servizi di amministrazione di sistema affidati in *outsourcing* il titolare o il responsabile del trattamento devono conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.
Verifica delle attività: l´operato degli amministratori di sistema deve essere oggetto, **con cadenza almeno annuale,** di un´attività di verifica da parte dei titolari o dei responsabili del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.
Registrazione degli accessi: devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) **ai sistemi di elaborazione** e agli **archivi elettronici** da parte degli amministratori di sistema. Le registrazioni (*access log*) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.
Le registrazioni devono comprendere i **riferimenti temporali** e la **descrizione dell´evento che le ha generate** e devono essere **conservate** per un congruo periodo, non inferiore a sei mesi.

4 QUERY E ACCESSI ALLE BANCHE DATI

Tipologia dati - Articolo 4 (Definizioni)
Ai fini del Regolamento UE 2016/679 s'intende per:
1) «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
2) «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione
o la distruzione.

Quantità di informazioni e tempi di conservazione - Articolo 5 (Principi applicabili al trattamento di dati personali)
I dati personali sono:
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («**minimizzazione** dei dati»);
e**) 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**»)

Consensi, *blacklist* e gestione diritti - Articolo 7 (Condizioni per il consenso)
1. Qualora il trattamento sia basato sul consenso, il **titolare del trattamento** deve essere in grado di **dimostrare che l'interessato ha prestato il proprio consenso** al trattamento dei propri dati personali.
3. L'interessato ha il diritto di **revocare il proprio consenso** in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di prestare il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.

Utenti abilitati e nomine autorizzati - **Articolo 29 (Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento)**
Il responsabile del trattamento, o **chiunque agisca** sotto la sua autorità o sotto quella del titolare del trattamento, che abbia **accesso a dati personali** non può trattare tali dati se non è **istruito** in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

5 AUTORIZZATI AL TRATTAMENTO

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

GESTISCI BENE LE TUE PASSWORD

- **Utilizza password diverse per account diversi** (e-mail, social network, servizi digitali di varia natura, ecc.). In caso di «furto» di una password si evita così il rischio che anche gli altri profili che ti appartengono possano essere facilmente violati.
- Altra accortezza importante è quella di **NON utilizzare password già utilizzate in passato**.
- Occorre poi ricordare che le eventuali **password temporanee** rilasciate da un sistema o da un servizio informatico vanno sempre immediatamente cambiate, scegliendone una personale.

CONSERVA CON CURA LE TUE PASSWORD

- **Non scrivere mai le password su biglietti** che poi magari conservi nel portafoglio o indosso, o che puoi distrattamente lasciare in giro, oppure in file non protetti sui tuoi dispositivi personali (computer, smartphone o tablet).
- **Evita sempre di condividere le password** via e-mail, sms, social network, instant messaging, ecc.. Anche se le comunichi a persone conosciute, le credenziali potrebbero essere diffuse involontariamente a terzi o «rubate» da malintenzionati.
- Se usi pc, smartphone e altri dispositivi che non ti appartengono, **evita sempre che possano conservare in memoria le password da te utilizzate**.

IMPOSTA BENE LA TUA PASSWORD

Una buona password:

- **deve essere abbastanza lunga**: almeno 8 caratteri, anche se più aumenta il numero dei caratteri più la password diventa "robusta" (si suggerisce intorno ai 15 caratteri);
- **deve contenere caratteri di almeno 4 diverse tipologie**, da scegliere tra: lettere maiuscole, lettere minuscole, numeri, caratteri speciali (cioè punti, trattino, underscore, ecc.);
- **non deve contenere riferimenti personali facili da indovinare** (nome, cognome, data di nascita, ecc.). Non deve nemmeno contenere riferimenti al nome utente (detto anche user account, alias, user id, user name);
- **meglio evitare che contenga parole "da dizionario"**, cioè parole intere di uso comune: è meglio usare parole di fantasia oppure parole "camuffate" per renderle meno comuni, magari interrompendole con caratteri speciali (ad esempio: caffè può diventare caf-f3). Esistono infatti software programmati per tentare di indovinare e rubare le password provando sistematicamente tutte le parole di uso comune nelle varie lingue, e con questa accortezza si può rendere il loro funzionamento più complicato;
- **andrebbe periodicamente cambiata**, soprattutto per i profili più importanti o quelli che usi più spesso (e-mail, e-banking, social network, ecc.).

5 AUTORIZZATI AL TRATTAMENTO

Il **phishing** è una tecnica illecita utilizzata per **appropriarsi di informazioni riservate relative a una persona o a un'azienda** - username e password, codici di accesso (come il PIN del cellulare), numeri di conto corrente, dati del bancomat e della carta di credito – con l'intento di compiere operazioni fraudolente.

La truffa avviene di solito via e-mail, ma possono essere utilizzati anche sms, chat e social media. Il «ladro di identità» si presenta, in genere, come un soggetto autorevole (banca, gestore di carte di credito, ente pubblico, ecc.) che invita a fornire dati personali per risolvere particolari problemi tecnici con il conto bancario o con la carta di credito, per accettare cambiamenti contrattuali o offerte promozionali, per gestire la pratica per un rimborso fiscale o una cartella esattoriale, ecc..

In genere, **i messaggi di phishing invitano a fornire direttamente i propri dati personali, oppure a cliccare un link che rimanda ad una pagina web dove è presente un form da compilare.** I dati così carpiti possono poi essere utilizzati per fare acquisti a spese della vittima, prelevare denaro dal suo conto o addirittura per compiere attività illecite utilizzando il suo nome e le sue credenziali.

a sconosciuti.

E' bene ricordare che, in generale, banche, enti pubblici, aziende e grandi catene di vendita non richiedono informazioni personali attraverso e- mail, sms, social media o chat: quindi, meglio evitare di fornire dati personali, soprattutto ditipo bancario, attraverso tali canali.

Se si ricevono messaggi sospetti, è bene **non cliccare sui link in essi contenuti e non aprire eventuali allegati**, che potrebbero contenere virus o programmi trojan horse capaci di prendere il controllo di pc e smartphone. Spesso dietro i nomi di siti apparentemente sicuri o le URL abbreviate che si trovano sui social media si nascondono link a contenuti non sicuri.

Una piccola accortezza consigliata è quella di posizionare sempre il puntatore del mouse sui link prima di cliccare: in molti casi si potrà così leggere in basso a sinistra nel browser il vero nome del sito cui si verrà indirizzati.

Phishing: attenzione ai «pescatori» di dati personali

Il buonsenso prima di tutto

Occhio agli indirizzi

I messaggi di phishing sono progettati per ingannare e spesso utilizzano imitazioni realistiche dei loghi o addirittura delle pagine web ufficiali di banche, aziende ed enti. Tuttavia, capita spesso che contengano anche **grossolani errori grammaticali, di formattazione o di traduzione da altre lingue.**
E' utile **anche prestare attenzione al mittente** (che potrebbe avere un nome vistosamente strano o eccentrico) o al suo indirizzo di posta elettronica (che spesso appare un'evidente imitazione di quelli reali).
Meglio diffidare dei **messaggi con toni intimidatori**, che ad esempio contengono minacce di chiusura del conto bancario o di sanzioni se non si risponde immediatamente: possono essere subdole strategie per spingere il destinatario a fornire informazioni personali.

Proteggersi è meglio

E' utile installare e tenere aggiornato sul pc o sullo smartphone un **programma antivirus che protegga anche dal phishing.** Programmi e gestori **di posta elettronica** hanno spesso **sistemi di protezione** che indirizzano automaticamente nello **spam** la maggior parte dei messaggi di phishing: è bene controllare che siano attivati e verificarne le impostazioni. Meglio **non memorizzare dati personali e codici di accesso nei browser** utilizzati per navigare online. In ogni caso, è buona prassi **impostare password alfanumeriche complesse**, cambiandole spesso e scegliendo credenziali diverse per ogni servizio utilizzato: banca online, e-mail, social network, ecc. *[vedi anche la scheda del Garante con i consigli per gestire le password in sicurezza]*, a meno di disporre di sistemi di autenticazione forte (*strong authentication*).

www.garanteprivacy.it

6 MISURE DI SICUREZZA

Articolo 32 - Sicurezza del trattamento

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto **misure tecniche e organizzative adeguate** per **garantire** un **livello di sicurezza adeguato al rischio**, 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.

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei **rischi presentati dal trattamento** che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

3. L'adesione a un **codice di condotta** approvato di cui all'articolo 40 o a un meccanismo di **certificazione** approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.

4. Il titolare del trattamento e il responsabile del trattamento fanno sì che **chiunque agisca sotto la loro autorità e abbia accesso a dati personali** non tratti tali dati se non è **istruito** in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

7 DATA BREACH

ARTICOLO 4 – DEFINIZIONI

Ai fini del Regolamento UE 2016/679 s'intende per:

12) «**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.

Articolo 33 - Notifica di una violazione dei dati personali all'autorità di controllo

1. In caso di **violazione dei dati personali**, il titolare del trattamento **notifica la violazione all'autorità di controllo competente** a norma dell'articolo 55 **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**. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

3. La notifica di cui al paragrafo 1 deve almeno:

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.

4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

5. Il titolare del trattamento **documenta** qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

Articolo 34 - Comunicazione di una violazione dei dati personali all'interessato

1. 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.

2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive 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).

8 DATACENTER EXTRA-UE

I **trasferimenti di dati personali verso Paesi non appartenenti allo Spazio Economico Europeo** (SEE, ossia UE + Norvegia, Liechtenstein, Islanda) o verso un'organizzazione internazionale sono consentiti a condizione che l'**adeguatezza** del Paese terzo o dell'organizzazione sia riconosciuta tramite **decisione della Commissione europea** (art. 45 del Regolamento UE 2016/679).

In assenza di tale decisione, il trasferimento è consentito ove il titolare o il responsabile del trattamento forniscano **garanzie adeguate** che prevedano diritti azionabili e mezzi di ricorso effettivi per gli interessati (art. 46 del Regolamento UE 2016/679).

Al riguardo, possono costituire garanzie adeguate:
- **senza autorizzazione da parte del Garante**:
• gli **strumenti giuridici** vincolanti ed esecutivi tra soggetti pubblici (art. 46, par. 2, lett. a);
• le norme vincolanti d'impresa (art. 46, par. 2, lett. b)
• le **clausole tipo** (art. 46, par. 2, lett. c e lett. d)
• i **codici di condotta** (art. 46, par. 2, lett. e)
• i **meccanismi di certificazione** (art. 46, par. 2, lett. f)
- **previa autorizzazione del Garante**:
• le **clausole contrattuali** ad hoc (art. 46, par. 3, lett. a)
• gli **accordi amministrativi** tra autorità o organismi pubblici (art. 46, par. 3, lett. b)

In assenza di ogni altro presupposto, è possibile trasferire i dati personali in base ad alcune deroghe che si verificano in specifiche situazioni (art. 49 del Regolamento UE 2016/679).

Articolo 45 - Decisioni di adeguatezza

La Commissione europea può stabilire, valutati gli elementi indicati nell'art. 45, par. 2 del Regolamento UE 2016/679 e sulla base di un **procedimento** che prevede il parere del Comitato europeo per la protezione dei dati, che il **Paese terzo** (ma anche un territorio o un settore specifico al suo interno) o **l'organizzazione internazionale garantiscano un livello di protezione adeguato** e che pertanto è possibile trasferirvi dati personali. Il Regolamento prevede un'attività di monitoraggio da parte della Commissione mediante **riesame delle decisioni a cadenza periodica**, almeno ogni quattro anni. Tale attività può concludersi con una modifica della decisione o in altre circostanze con la sospensione o persino con la sua revoca, (art. 45, paragrafi 3-5 del Regolamento UE 2016/679).

MAGGIORE CONSAPEVOLEZZA

Rapporto Osservatorio sugli Attacchi Digitali (OAD) in Italia 2023

Nel corso del **2022**, una **percentuale significativa** dei sistemi informatici dei soggetti in esame è stata presa di mira da **attacchi di vario genere**.

Più della metà dei partecipanti ha indicato **vulnerabilità tecniche**, che riguardano l'**applicazione web**, la **piattaforma web** e i **dispositivi degli utenti**.

Una percentuale minore ha evidenziato anche delle vulnerabilità legata agli **utenti**, sia quelli **finali** sia quelli **con privilegi elevati**, come amministratori di sistemi, sistemisti e fornitori.

La principale minaccia, che rappresenta quasi un quinto degli attacchi più gravi segnalati dai partecipanti, è costituita da **componenti software obsoleti e vulnerabili**.

Sommando questo dato alla vulnerabilità causata da una **progettazione non sicura dei software** e alla **cattiva configurazione della sicurezza digitale dei propri siti web**, si arriva a quasi il cinquanta percento delle cause di attacchi gravi ai sistemi.

L'**OAD 2023** sottolinea come gli impatti degli attacchi più gravi alle piattaforme web possano essere suddivisi in due categorie principali: impatti tecnici e impatti economici.

La netta maggioranza dei partecipanti al sondaggio ha registrato **impatti tecnici significativi**, con un disservizio che ha superato i due giorni, provocando notevoli disagi in ambito informatico.

Nel dettaglio, un quarto delle aziende e degli enti coinvolti ha risentito di **impatti economici rilevanti**, i cui costi tecnici supplementari hanno influito pesantemente sul bilancio complessivo delle rispettive organizzazioni.

Sul versante economico, invece, i costi aggiuntivi generati da attacchi e falle nella sicurezza, hanno inciso notevolmente sul bilancio dei sistemi informativi delle realtà prese in considerazione e, in alcuni casi, hanno avuto **ripercussioni significative sull'intero bilancio dell'azienda o dell'ente coinvolto.**

Rapporto OAD 2023 (oadweb.it)

L'impresa "F.O.R.T.E." è CONSAPEVOLE dei RISCHI

- Ciascun componente della struttura organizzativa deve essere NODO di DIFESA degli *asset* informatici dell'impresa

- Importante la figura del COMPLIANCE OFFICER o del TEAM multidisciplinare/trasversale

- La COMPLIANCE PRIVACY attribuisce valore al **sito web** e all'**azienda**

- Aspetto REPUTAZIONALE: anche CLIENTI/UTENTI danno valore all'azienda privacy *compliant* perché più affidabile

L'impresa "F.O.R.T.E." è ANTROPOCENTRICA

Articolo **41**

L'iniziativa economica privata è libera.
Non può svolgersi in contrasto con l'utilità sociale o in modo da arrecare danno… alla sicurezza, alla libertà, alla dignità umana.

La chiave per il governo dell'innovazione e protezione dei dati è fornito dall'APPROCCIO ANTROPOCENTRICO.
Anche per i siti web aziendali vale lo stesso principio:
la PERSONA e i suoi diritti **al centro di tutto**.

GRAZIE PER L'ATTENZIONE