

Ciclo di webinar su digitale, agricoltura e mondo rurale

Agricoltura digitale: soluzioni e opportunità

Agricoltura Digitale – Impatto privacy in azienda

25.06.2020



Avv. Giovanni Bonato

Data Protection Officer

gbonatolegal@gmail.com

Regolamento 679/16 – GDPR COME SISTEMA DI GESTIONE

L'art. 25 GDPR : Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.

Articolo 32 : Sicurezza del Trattamento

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

Misure di sicurezza

Le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" del trattamento (art. 32, paragrafo 1).

[...] Per lo stesso motivo, non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza (ex art. 33 Codice) poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati. Si richiama l'attenzione anche sulla possibilità di utilizzare l'adesione a specifici codici di condotta o a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate.

GDPR come SISTEMA DI GESTIONE, quindi adottiamo approccio idoneo alla singola realtà aziendale.

DATO PERSONALE

Quando si parla di privacy parliamo di dati relativi alle Persone Fisiche

«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

- Questi sono, ad esempio, dati personali:
- Nome, cognome e soprannome
- Indirizzo di casa
- Registrazione vocale
- Impronta digitale
- Conto bancario
- etc.



TRATTAMENTO

Il Regolamento UE 679/2016 (GDPR) dà una nozione di trattamento del dato personale molto ampia:

ART. 4, N. 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;

ATTORI DELLA PRIVACY

Interessato

La persona fisica cui si riferiscono i dati personali.

Titolare del Trattamento

La persona fisica, la società, l'associazione o un'altra entità che controlla il trattamento dei dati personali ed è autorizzata a prendere decisioni essenziali sulle **finalità e modalità** di tale trattamento, comprese le **misure di sicurezza** applicabili.

Autorizzato

soggetto che opera sotto l'autorità diretta del titolare o del responsabile

Responsabile del Trattamento

La persona fisica, la società, l'associazione o l'organizzazione **a cui il Titolare ha affidato – dettando finalità e modalità - l'attività specifica di gestione e controllo** dei dati personali, in base all'esperienza e/o alle competenze pertinenti in materia.

DPO (Data Protection Officer)

Il professionista con conoscenze specialistiche sulla legislazione e sulle pratiche in materia di protezione dei dati.

Egli è designato dal Titolare / Responsabile in tre occasioni:

Il trattamento è effettuato da un'autorità pubblica

Il trattamento è su larga scala e coinvolge dati particolari

Il trattamento richiede un controllo regolare e sistematico degli Interessati

Terzo

La persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati sotto l'autorità diretta del titolare o del responsabile

Titolare del trattamento (azienda Alfa)

Responsabile del trattamento

es. Consulente del lavoro,
commercialista, Azienda Resp IT

Terzi

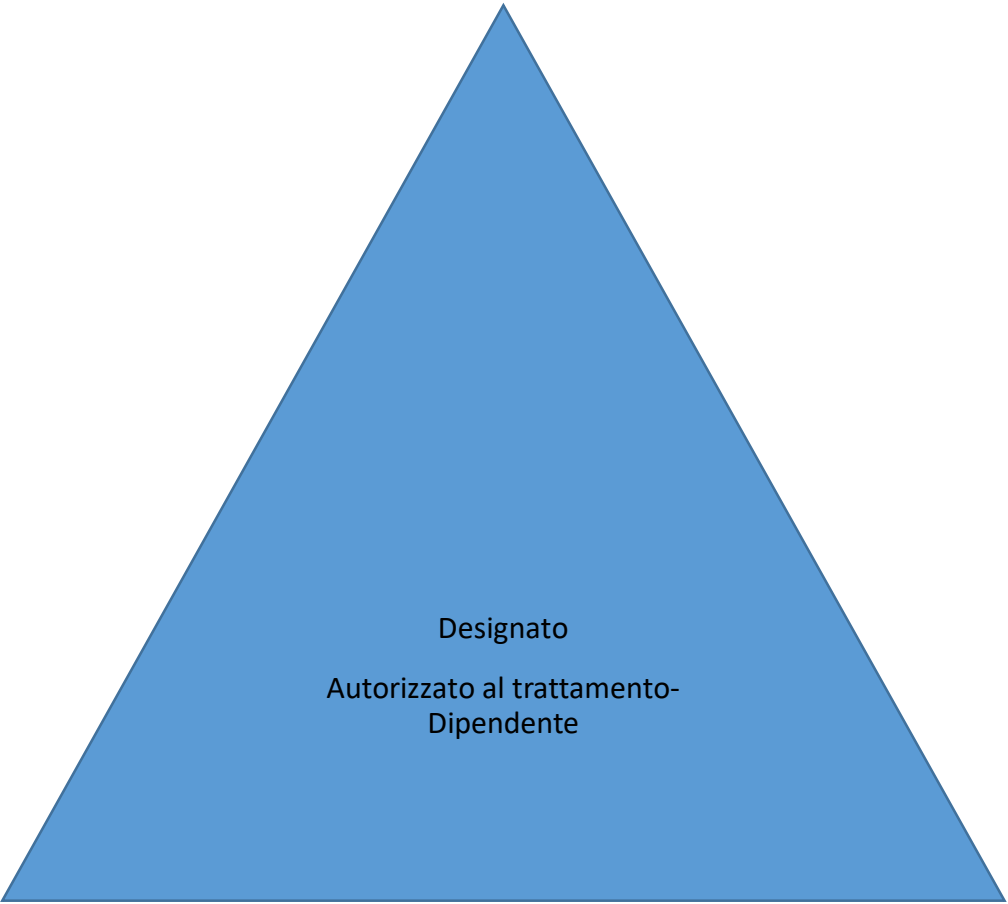
INPS -INAIL

DPO

Designato

Autorizzato al trattamento-
Dipendente

Interessato (persona fisica)



ADEMPIMENTI

- Definizione trattamenti essenziali:

1) Dipendenti:

- informativa ex art. 13: informo il dipendente sulle modalità e finalità del trattamento dei suoi dati ai fini dello svolgimento del rapporto di lavoro;
- autorizzazione al trattamento: comunico al dipendente delle regole precise per il trattamento dei dati in azienda (importante per il reparto amm.ne, commerciale, processo attivo e passivo).

2) Fornitori:

- Informativa ex art. 13: informo il fornitore sulle modalità e finalità del trattamento dei suoi dati ai fini dello svolgimento del rapporto di fornitura;
- Se il fornitore tratta dati per nostro conto va nominato responsabile del trattamento ex art. 28 GDPR (es consulente del lavoro);

3) Clienti:

- Informativa ex art. 13: informo il cliente sulle modalità e finalità del trattamento dei suoi dati ai fini della vendita/ servizio.

- Registro dei trattamenti;
- Analisi dei rischi: analisi dei trattamenti, misure tecniche e organizzative, in considerazione di tre fattori:
 - a) Riservatezza: divulgazione non autorizzata;
 - b) Integrità: alterazione non autorizzata;
 - c) Disponibilità: distruzione o perdita non autorizzata.
- Definizione di procedure (data breach – esercizio dei diritti dell'interessato);
- Security: sistemi di *DB centralizzati su Server*, oppure in *Cloud certificati* (localizzati nella UE), dotati di firewall con sistemi antintrusione Intrusion Detection System (IDP) e Intrusion Prevention System (IPS) e sistemi di backup collaudati e ben configurati in funzione di un'**analisi dei rischi** fatta a monte.



**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

SCHEDA REGISTRO DEI TRATTAMENTI *[per i contenuti vedi Faq sul registro delle attività di trattamento: <https://www.garanteprivacy.it/regolamentoue/registro>]*

TITOLARE/CONTITOLARE/RAPPRESENTANTE DEL TITOLARE *[inserire la denominazione e i dati di contatto]*

RESPONSABILE DELLA PROTEZIONE DEI DATI *[inserire la denominazione e i dati di contatto]*

TIPOLOGIA DI TRATTAMENTO	FINALITA' E BASI LEGALI DEL TRATTAMENTO	CATEGORIE DI INTERESSATI	CATEGORIE DI DATI PERSONALI	CATEGORIE DI DESTINATARI <i>[Indicare eventuali responsabili del trattamento o altri titolari cui i dati siano comunicati]</i>	TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI <i>[Indicare il Paese terzo o l'organizzazione internazionale cui i dati sono trasferiti e le "garanzie" adottate ai sensi del capo V del RGPD]</i>	TERMINI ULTIMI DI CANCELLAZIONE PREVISTI	MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

Valutazione d'impatto

Analisi d'Impatto		
Riservatezza	Integrità	Disponibilità
Medio	basso	basso
Valutazione di Impatto Globale		Medio

Probabilità occorrenza minacce

Area di valutazione	Probabilità	
	Livello	Punteggio
Trattamenti/Procedure relative al trattamento dati personali	Basso	1
Parti/Persone coinvolte nel trattamento dei dati personali	Medio	2
Settore di attività e portata del trattamento	Basso	1
Probabilità di accadimento	Basso (4)	

Valutazione del rischio sul trattamento

		Livello d'impatto		
		Basso	Medio	Alto / Molto Alto
Probabilità che si verifichi una minaccia	Basso		X	
	Medio			
	Alto			

ATTIVITA' DI VENDITA ON – LINE E IMPATTO GDPR

SITO INTERNET

SITO INTERNET: indice rivelatore di compliance

Rispetto a:

- a) Autorità (Garante e Gdf);
- b) Competitor;
- c) Utenti del web.

CHI SONO GLI UTENTI

- Dati di utenti (clienti e potenziali clienti) acquisiti mediante il web;
- Dati degli utenti (clienti e potenziali clienti) già acquisiti per altra via (rapporto commerciale) che voglio contattare;

NEL WEB...

Dati di navigazione. I sistemi informatici e le procedure software preposte al funzionamento dei siti web acquisiscono, nel corso del loro normale esercizio, alcuni dati personali la cui trasmissione è implicita nell'uso dei protocolli di comunicazione di Internet. In questa categoria di dati rientrano, ad esempio, gli indirizzi IP o 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 ed altri parametri relativi al sistema operativo e all'ambiente informatico dell'utente. Questi dati vengono utilizzati al solo fine di ricavare informazioni statistiche anonime sull'uso del sito e per controllarne il corretto funzionamento e vengono cancellati immediatamente dopo l'elaborazione.

Dati forniti volontariamente dall'Utente L'invio di posta elettronica agli indirizzi indicati nel Sito - facoltativo, esplicito e volontario - comporta la successiva acquisizione dell'indirizzo e-mail, necessario per rispondere alle richieste, nonché degli ulteriori dati personali eventualmente comunicati.

Cookie Per ogni informazione in ordine all'utilizzo dei cookie da parte del Sito, accedi all'apposita informativa [cliccando qui](#).

RAPPORTO CON WEB AGENCY VA FORMALIZZATO

Art. 4 GDPR : Il responsabile del trattamento è definito dal GDPR come la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che tratta dati personali per conto del titolare del trattamento.

Art. 28 GDPR : [...] 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 ed organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato”.

MARKETING..ATTENZIONE AL CONSENSO!

LA REGOLA

Art 130 del Codice della Privacy, ai co. 1 e 2 sancisce che “1. [...] l'uso di sistemi automatizzati di chiamata o di comunicazione di chiamata senza l'intervento di un operatore per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale è consentito con il consenso del contraente o utente[...].

2. La disposizione di cui al comma 1 si applica anche alle comunicazioni elettroniche, effettuate per le finalità ivi indicate, mediante posta elettronica, telefax, messaggi del tipo Mms (Multimedia Messaging Service) o Sms (Short Message Service) o di altro tipo.”

ATTENZIONE ALL'ECCEZIONE!

Art. 130 co. 4 Codice privacy (che di fatto va ad attuare quanto previsto nell'art. 13 della direttiva 2002/58/CE - regolamento sulla vita privata e le comunicazioni elettroniche) *“Fatto salvo quanto previsto nel comma 1, se il titolare del trattamento utilizza, a fini di vendita diretta di propri prodotti o servizi, le coordinate di posta elettronica fornite dall'interessato nel contesto della vendita di un prodotto o di un servizio, può non richiedere il consenso dell'interessato, sempre che si tratti di servizi analoghi a quelli oggetto della vendita e l'interessato, adeguatamente informato, non rifiuti tale uso, inizialmente o in occasione di successive comunicazioni. L'interessato, al momento della raccolta e in occasione dell'invio di ogni comunicazione effettuata per le finalità di cui al presente comma, è informato della possibilità di opporsi in ogni momento al trattamento, in maniera agevole e gratuitamente.”*

Art. 6 GDPR – Base giuridica 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.

Considerando (47)

I legittimi interessi di un titolare del trattamento, compresi quelli di un titolare del trattamento a cui i dati personali possono essere comunicati, o di terzi possono costituire una base giuridica del trattamento, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato, tenuto conto delle ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento.

Ad esempio, potrebbero sussistere tali legittimi interessi quando esista una relazione pertinente e appropriata tra l'interessato e il titolare del trattamento, ad esempio quando l'interessato è un cliente o è alle dipendenze del titolare del trattamento [...].

[...] Può essere considerato legittimo interesse trattare dati personali per finalità di marketing diretto

Marketing di prossimità (Soft spam) per propri clienti

L'interessato è già cliente del titolare:

- la [base giuridica](#) può consistere nei [legittimo interesse del titolare](#) e quindi non occorre il consenso per l'invio delle comunicazioni pubblicitarie (art. 13(2) [direttiva e-Privacy](#)).

Tale importante eccezione è subordinata alla presenza dei seguenti requisiti:

- vale solo per la trasmissione di **messaggi per posta elettronica**;
- la **mail** deve essere quella **indicata nel contesto della vendita di un prodotto o servizio**;
- i messaggi devono essere inviati a fini di vendita diretta di **prodotti e/o servizi forniti dal titolare** (e non da terzi);
- il prodotto o il servizio devono essere **analoghi a quelli già acquistati** dall'interessato;
- il destinatario non deve aver rifiutato all'inizio o nel corso di ulteriori comunicazioni tale invio di comunicazioni promozionali;
- il destinatario deve avere la **possibilità di opporsi** al trattamento dei dati in ogni momento, gratuitamente e in maniera semplice.

PROFILAZIONE

ART 4 paragrafo 1 n. 4) GDPR:

«Profilazione» qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali **per valutare determinati aspetti personali relativi a una persona fisica**, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

MODALITA'

- OFFLINE: il consenso va richiesto nel modulo per il rilascio (es tessera fedeltà);
- ONLINE: il consenso deve essere richiesto nel momento in cui si accede al sito

COOKIES

CONSIDERANDO N. 30 GDPR

Le persone fisiche possono essere associate a **identificativi online** prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, a marcatori temporanei (cookies) o a identificativi di altro tipo, come 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

BANNER COOKIES

Come deve essere strutturato?

- Deve indicare le varie tipologie di cookie utilizzate;
- Deve consentire la scelta tra le diverse tipologie;
- NON deve presentare caselle già spuntate (salvo cookies tecnici in assenza dei quali il sito non funziona)
- Deve esserci un link per informazioni complete sui cookies;

Fac simile

Questo sito web utilizza i cookie

Utilizziamo i cookies per personalizzare contenuti ed annunci, per fornire funzionalità dei social media e per analizzare il nostro traffico. Condividiamo inoltre informazioni sul modo in cui utilizza il nostro sito con i nostri partner che si occupano di analisi dei dati web e pubblicità, i quali potrebbero combinarle con altre informazioni che lei ha fornito o che hanno raccolto dal suo utilizzo dei loro servizi.

Acconsenta ai nostri cookie se continua ad utilizzare il nostro sito web.

☒necessario ☐ preferenze ☐ statistiche ☐ marketing [Mostra dettagli](#)

ADEMPIMENTI SITO

- Policy privacy;
- Cookies policy;
- Informativa news letter – predisposizione di policy autonoma;
- Informativa «contatti» - predisposizione informativa e consenso per marketing;
- Informativa «lavora con noi» - predisposizione informativa ad hoc e consenso;

MINIMIZZAZIONE E NECESSARIETA'!!

DATA BREACH

“Data breach” secondo il Regolamento UE 679/2016 (che tratta la materia agli articoli 33 e 34), è una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso ai dati personali trasmessi, conservati o comunque trattati.

Per minimizzare l’impatto di una violazione dei dati è importante dotarsi di un adeguato modello organizzativo che affronti in maniera adeguata tre elementi: valutazione dei rischi; organizzazione aziendale; sicurezza informatica.

CONSEGUENZE

- **pagamento di sanzioni** (comminate sulla base della normativa Privacy);
- **Danno da responsabilità civile**, vds 82 del Regolamento: *“Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento”*
- **danno reputazionale** (vds opinione pubblica e mercati, come hanno reagito al caso Cambridge Analytica).

Caso. Società fornitrice di un servizio di messaggistica online, ha recentemente subito un attacco nel quale sono state **trafugate le credenziali di accesso (nomi utente e password) di centinaia di migliaia di utenti** iscritti alla propria piattaforma.

Garante tedesco: società è stata multata per un totale di 20.000€ con l'attenuante di "spirito di collaborazione e trasparenza dell'azienda nei confronti delle autorità".

Caso Catena alberghiera è ancora più cocente.

L'azienda ha comunicato al garante per la Privacy nazionale un furto di dati ai danni di oltre **500.000 utenti**.

Anche in questo caso l'azienda ha cercato di risolvere la crisi **offrendo il rimborso agli utenti violati**, attivato un **call center** e un **centro di crisi** a cui è possibile rivolgersi per chiedere informazioni sulla possibile violazione dei propri dati personali.

Le spese sostenute dall'azienda non possono però essere equiparate al **danno registrato sul fronte reputazionale**:

- il crollo dei titoli del Brand alla Borsa di New York, segno evidente della mancanza di fiducia accordata.
- La **conseguenza del Data Breach** si è registrata sul lungo periodo portando ad un'impennata del 3.400% delle ricerche on line relative alla query "xxx data breach" che si colloca al 4° posto tra le parole correlate alla ricerca generica xxx, il che significa che **il terzo argomento collegato alla catena di alberghi è proprio il furto di dati personali**.

COME REAGIRE

Reagire al data breach implica avere consapevolezza che la violazione si sia verificata. L'avvio delle 72 ore parte dal momento in cui l'azienda sia venuta a conoscenza della violazione dei dati personali.

- 1) PREVENZIONE: un processo di data breach deve essere preceduto da un'analisi delle vulnerabilità del proprio sistema IT;
- 2) ATTENZIONE AI CONTRATTI: La tempestività è determinata dal rapporto e dalla comunicazione tra:
 - *controller e processor (titolare e responsabile) – previsione di clausole specifiche;*
 - *controller e persone autorizzate al trattamento – autorizzazione al trattamento, canali informativi chiari, formazione;*
 - *tra controller ed interessati – chiare modalità di esercizio dei diritti.*

3) Istituzione di un comitato esegue la valutazione del data breach e ne analizza i risultati, in funzione del rischio e delle possibilità di mitigazione e rimedi perseguibili dall'azienda o dagli interessati;

...in assenza di misure preventive l'eventuale valutazione da parte dell'Autorità sarà sicuramente meno indulgente e la sanzione eventualmente imposta più elevata

VALUTAZIONE DELLA VIOLAZIONE

Valutazione della violazione varieranno a seconda di:

- tipo di violazione e natura dei dati violati (es. violazione di riservatezza, di accessibilità o di integrità dei dati; dati sanitari, documenti di identità o numeri di carte di credito);
- la facilità con cui potrebbero essere identificati gli interessati (es. l'aggressione riguarda dati identificativi o dati personali non direttamente identificativi; era previsto l'utilizzo di tecniche di pseudonimizzazione o crittografia);
- la gravità delle conseguenze sugli individui in termini di potenziali danni (es. i dati sono stati inviati erroneamente a un fornitore di fiducia o sono stati sottratti da un terzo sconosciuto);
- speciali caratteristiche e numero degli individui interessati (es. bambini o anziani; violazione massiccia o individuale);
- particolari caratteristiche del titolare (es. ambito di attività economico o sanitario; contatto frequente con dati sensibili).

COSA FARE IN CASO DI VIOLAZIONE DEI DATI PERSONALI?

Il titolare del trattamento (soggetto pubblico, impresa, associazione, partito, professionista, ecc.) **senza ingiustificato ritardo** e, ove possibile, **entro 72 ore dal momento in cui ne è venuto a conoscenza**, deve notificare la violazione al Garante per la protezione dei dati personali **a meno che sia improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche.**

Il responsabile del trattamento che viene a conoscenza di una eventuale violazione è tenuto a informare tempestivamente il titolare in modo che possa attivarsi.

NOTIFICA AL GARANTE

Le notifiche al Garante effettuate oltre il termine delle 72 ore devono essere accompagnate dai motivi del ritardo.

Inoltre, se la violazione comporta un rischio elevato per i diritti delle persone, il titolare deve comunicarla a tutti gli interessati, utilizzando i canali più idonei, a meno che abbia già preso misure tali da ridurre l'impatto.

Il titolare del trattamento, a prescindere dalla notifica al Garante, **documenta** tutte le violazioni dei dati personali, ad esempio predisponendo un apposito registro. Tale documentazione consente all'Autorità di effettuare eventuali verifiche sul rispetto della normativa.

FAC SIMILE MADALITA' OPERATIVE

- 1) In ipotesi di incidente che comporti la perdita di disponibilità, integrità o riservatezza dei dati personali del cui trattamento sia Titolare ALFA, il responsabile IT, unitamente al Designato Privacy, provvederà immediatamente alla messa in sicurezza del sistema, isolando, ove possibile, la porzione eventualmente oggetto di infezione e verificando:
 - a) la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati coinvolti, le categorie e il numero approssimativo di registrazioni dei dati personali in questione nonché i sistemi e le infrastrutture IT coinvolte;
 - b) le probabili conseguenze derivanti dalla violazione dei dati personali;
 - c) 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; comunicando le predette informazioni, contestualmente, al titolare del trattamento ed al reparto amministrativo.

2) qualora il Data Breach avvenga presso un fornitore nominato Responsabile del Trattamento, questi dovrà entro 24h dall'incidente fornire a ALFA le informazioni di cui al punto 1);

3) il Titolare del trattamento, consultato il Designato Privacy notificherà la violazione – compilando il modulo “VIOLAZIONE DI DATI PERSONALI – MODELLO DI NOTIFICA AL GARANTE” – al Garante per la Protezione dei Dati Personali in Roma senza ingiustificato ritardo e, ove possibile, entro 72 (settantadue) 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.** Con la notificazione comunicherà altresì il nome e i recapiti del punto di contatto, designato tra i ruoli di riferimento aziendali, presso cui ottenere più informazioni.

Qualora la notifica all'autorità di controllo non sia effettuata entro 72 (settantadue) ore, sarà corredata dai motivi del ritardo

4) Alla luce delle verifiche operate, se:

a) la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche;

b) non siano state messe in atto (ovvero non erano applicate ai dati personali oggetto della violazione), prima dell'incidente, adeguate misure tecniche e organizzative di protezione, tali da rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi (a titolo esemplificativo, la crittografia);

c) successivamente all'incidente, non siano state adottate misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

Il titolare del trattamento comunicherà agli interessati coinvolti la violazione dei loro dati personali, per il tramite del reparto amministrativo e con modalità tracciabili di corrispondenza, senza ingiustificato ritardo.

Nei casi in cui detta comunicazione richiederebbe sforzi sproporzionati, si procederà ad una comunicazione pubblica o a una misura simile, tramite la quale gli interessati saranno informati con analoga efficacia.

5) Anche al di fuori dei casi precedenti, il Titolare del trattamento, per il tramite del responsabile IT e del reparto amministrativo, documenterà qualsiasi incidente che comporti la violazione dei dati personali compilando il modulo “REGISTRO DATA BREAH”, comprese le circostanze ad essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.